

# Informatiebeveiligings- en Privacybeleid (IBP)



Amersfoort, 2021, Versie 0.9

## Eigenschappen Document

Elk document binnen de Optimo dient duidelijk te worden voorzien van metadata, zoals versienummer en een classificatie.

Vul de gegevens in de onderstaande tabel in:

<b>Auteur</b>	Tjeerd de Bruijn
<b>Creatie datum</b>	14-08-2020
<b>Titel</b>	Optimo Informatiebeveiligings- en Privacybeleid

## Classificatie Document

Binnen Optimo hanteren wij de onderstaande classificaties. Privacygegevens worden standaard beschouwd als vertrouwelijk:

- Openbaar
- Intern gebruik
- Vertrouwelijk
- Geheim

<b>Classificatie</b>	Openbaar
----------------------	----------

## Versiebeheer

Hieronder het versiebeheer voor dit document:

Versie	Omschrijving	Datum	Auteur
0.1	Eerste versie document	14-08-2020	Tjeerd de Bruijn
0.2	Nieuwe versie	17-08-2020	Tjeerd de Bruijn
0.3	Nieuwe versie	18-08-2020	Ruud Miggelbrink
0.4	Nieuwe content	26-08-2020	Tjeerd de Bruijn
0.5	Hoofdstuk Accountmanagement aangepast	07-09-2020	Tjeerd de Bruijn
0.6	Titel document aangepast + nieuwe versie 2021	01-02-2021	Tjeerd de Bruijn
0.7	Review Optimo ISO team	19-10-2021	ISO team
0.8	Review met Intechrity	20-10-2021	ISO team

## Inleiding

Wij zijn Optimo. Optimo is een dienstverlenend bedrijf dat helpt bij het ontzorgen van het beheer en de inrichting van AFAS Profit en de interne processen van haar klanten. Verder is Optimo een gegevensverwerkend bedrijf dat op grote schaal klantdata verwerkt.

Bij deze dienstverlening hechten wij een groot belang aan de beveiliging van informatie en de bescherming van de privacy van zowel haar klanten en diens medewerkers als haar eigen medewerkers. Met dit document beschrijven wij hoe wij daar binnen Optimo invulling aan geven.

## Verantwoordelijkheid, doelstelling en doelgroep

Het gebruik van internet en verschillende bedrijfsmiddelen zijn noodzakelijk om de werkzaamheden voor onze klanten uit te voeren. Aan dit gebruik zijn risico's verbonden. Medewerkers van Optimo dienen zich bewust te zijn van deze risico's en dragen de verantwoordelijkheid om op de juiste manier, conform de door Optimo gestelde regels, te handelen. Eindverantwoordelijkheid voor het beleid inzake informatiebeveiliging en privacy ligt bij het management van Optimo.

Met betrekking tot informatiebeveiliging hanteert Optimo de volgende definitie:

### Informatiebeveiliging

*Informatiebeveiliging is het geheel van preventieve-, repressieve- en herstelmaatregelen alsmede procedures welke de beschikbaarheid, exclusiviteit en integriteit van alle vormen van informatie garanderen met als doel de continuïteit van de organisatie te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald, niveau te beperken.*

### Privacy

*Privacy informatiemanagement is een aanvulling op informatiebeveiligingsmanagement, met privacy specifieke maatregelen om het risico dat het recht op privacy van individuen wordt geschonden te beperken.*

De doelstelling van dit IBP-beleid luidt:

*'Het bieden van een raamwerk van beleidsuitgangspunten met betrekking tot de privacy, vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening, waarbinnen een evenwichtig (doeltreffend en doelmatig)*

*stelsel van onderling samenhangende maatregelen ontwikkeld wordt, teneinde de informatievoorziening te beschermen tegen interne en externe bedreigingen’.*

Het management, alle medewerkers én contractanten van Optimo dienen ervoor zorg te dragen, dat bij de inrichting van de organisatie, procedures, werkwijze en de daarbij gehanteerde informatiesystemen aan de in dit IBP-beleid geformuleerde beleidsuitgangspunten wordt voldaan.

Dit document is bestemd voor verschillende doelgroepen. Voor elk van die doelgroepen dient dit document een ander doel. Hieronder geven wij dit schematisch weer:

Doelgroep	Doel
Medewerkers (inclusief externen)	Bewust maken van het belang van informatiebeveiliging en richting en middelen geven om in het dagelijkse werk bij te dragen aan informatiebeveiliging.
Klanten	Inzicht geven in de maatregelen die Optimo neemt om de veiligheid van gegevens die wij voor hen beheren te beschermen.
Leveranciers	Inzicht geven in het beveiligingsbeleid van Optimo en daarmee inzicht geven in de beveiligingseisen die Optimo aan hen stelt.
Auditors	Inzicht geven in de opzet van informatiebeveiliging binnen Optimo zodat een beoordeling uitgevoerd kan worden.
Overige stakeholders	Ter informatie.

## Toepassingsgebied

Dit beleid is van toepassing op alle informatie die binnen de scope van het Optimo managementsysteem (OMS) wordt gecreëerd, ontvangen, verzonden of bewaard in de dienstverlening van Optimo aan klanten en de daarmee samenhangende contractuele verplichtingen. Het beleid en de uitwerking hiervan gelden voor alle medewerkers van Optimo die in aanraking komen met bovengenoemde informatie. Afwijkingen op beleid en uitwerking moeten gemeld worden, zodat het managementsysteem continue verbeterd kan worden. Daarnaast geldt dit beleid ook voor contractanten, die Optimo ondersteunen bij haar dienstverlening aan klanten.

## Uitwerking van dit beleid

Op basis van dit beleid worden risicoanalyses uitgevoerd en wordt een set van beheersingsmaatregelen (controls) gedefinieerd als basisbeveiligingsniveau, dat geldt als minimum voor de dienstverlening aan klanten.

## Controle werking en naleving van het beleid

Jaarlijks wordt de werking en de naleving van het beleid tijdens de directiebeoordeling intern geëvalueerd. Onderdeel van deze evaluatie betreft het opnieuw vaststellen van de risico's die Optimo loopt op het gebied van informatiebeveiliging en privacy.

Daarnaast wordt maandelijks in het Informatiebeveiliging en Privacy Overleg (IBPO) – waarbij in ieder geval de Controller, Security Officer en Functionaris Gegevensbescherming aanwezig zijn - de voortgang van geplande wijzigingen en verbetervoorstellen (het risicobehandelplan - RTP) besproken en besproken of er belangrijke wijzigingen te verwachten zijn met een IBP-risico (binnen wet- en regelgeving, wijzigingen binnen de organisatie, nieuw type dienstverlening enz.).

In het IBPO wordt de planning en het benodigde budget vastgesteld en toegekend. De notulen van het IBPO zijn een vast onderdeel van de vergaderingen van het MT.

Daarnaast voert een onafhankelijke derde partij jaarlijks een externe audit uit. Deze onafhankelijke derde partij is hiertoe bevoegd en deskundig. De rapportage met betrekking tot de externe audit is op aanvraag beschikbaar voor (potentiële) klanten.

## Beleidsuitgangspunten IBP

Met deze beleidsuitgangspunten geeft de directie van Optimo aan, op welke wijze zij wil dat met informatie- en privacy beveiliging omgegaan wordt.

Bij de verdere invulling van dit beleid dienen de volgende uitgangspunten gehanteerd te worden:

1. Optimo voldoet aantoonbaar aan de normen ISO 27001 (de standaard voor informatiebeveiliging) en ISO 27701 (de standaard voor privacy).
2. Informatie- en privacybeveiliging is opgezet met inachtneming van geldende wet- en regelgeving.
3. Bescherming van beveiliging van informatie en privacy zijn onderdeel van de algemene managementverantwoordelijkheden. Medewerkers zijn medeverantwoordelijk voor de bescherming van informatie en privacy.
4. Wanneer Optimo met leveranciers of partners een samenwerking aangaat wordt nadrukkelijk aandacht besteed aan informatiebeveiliging en privacy. Afspraken hierover worden schriftelijk vastgesteld en op de naleving wordt toegezien.
5. Optimo hanteert vaste in- en uitdiensttreedingsprocedures ten behoeve van het waarborgen van de vertrouwelijkheid van informatie van Optimo en haar klanten.
6. Optimo heeft passende maatregelen voor de fysieke beveiliging van mensen en middelen, waaronder vertrouwelijke informatie en apparatuur waarop die informatie is opgeslagen.

7. In samenhang met het geïmplementeerde Optimo Management System (OMS) waarborgt de uitvoering van dit beleidsplan een gestructureerde aanpak van en continue verbetering van informatiebeveiliging en privacy.

## Organisatie van informatiebeveiliging en privacy

Optimo zorgt met de inrichting van het Optimo Management Systeem (OMS) voor passende aandacht en sturing voor informatiebeveiliging en privacy. Optimo heeft een IBPO (Informatie Beveiliging en Privacy Overleg), waar het management, Security Officer en Privacy Officer (FG) aan deelnemen.

Binnen Optimo is de directie eindverantwoordelijk voor de informatiebeveiliging en privacy en voor de werking van het OMS. Het MT heeft een groot gedeelte van haar verantwoordelijkheid gedelegeerd aan het IBPO.

Binnen het IBPO zijn de volgende zaken belegd:

- Herziening en ter goedkeuring aan het MT voorleggen van (wijzigingen in) het informatiebeveiliging- en privacybeleid en de toegekende verantwoordelijkheden;
- Het signaleren van belangrijke wijzigingen en de voornaamste bedreigingen, waaraan de bedrijfsinformatie is blootgesteld;
- Bespreken, monitoren en evalueren van beveiligingsincidenten;
- Goedkeuring van plannen ter bevordering van informatiebeveiliging;
- Het doen van voorstellen voor toekenning van functies, rollen en verantwoordelijkheden voor informatiebeveiliging en privacy binnen Optimo;
- Het bereiken van overeenstemming over en het ondersteunen van initiatieven op het gebied van informatiebeveiliging in de gehele organisatie, bijvoorbeeld het bevorderen van het informatiebeveiliging- en privacy bewustzijn;
- Het beoordelen van auditresultaten en geconstateerde afwijkingen van beleid of procedures;
- Voorstellen voor het beschikbaar stellen van tijd, geld en middelen ten behoeve van informatiebeveiliging en privacy opstellen en indienen bij de verantwoordelijke.

De volgende rollen en de daarbij behorende verantwoordelijkheden hebben we binnen Optimo gedefinieerd:

Rol	Verantwoordelijkheden
<b>Management team (MT)</b>	Het managementteam heeft als verantwoordelijkheid: <ul style="list-style-type: none"> <li>• Strategische invulling en sturing van het OMS;</li> <li>• Het jaarlijks evalueren van het OMS.</li> </ul>
<b>IBP(O)</b>	Het IBP(O) heeft als verantwoordelijkheid: <ul style="list-style-type: none"> <li>• Tactische invulling en sturing van het OMS;</li> <li>• Het bewaken van operationele activiteiten van het OMS.</li> </ul>

<b>Privacy Officer (FG)</b>	Het is de verantwoordelijkheid van de Privacy Officer: <ul style="list-style-type: none"> <li>• Operationele en controlerende invulling en sturing van het OMS ten aanzien van PII.</li> </ul>
<b>Security Officer (SO)</b>	Het is de verantwoordelijkheid van de Security Officer: <ul style="list-style-type: none"> <li>• Operationele invulling en sturing van het OMS.</li> </ul>

## Scheiding van taken

Bij Optimo kan er in beginsel niemand autorisaties hebben om een gehele cyclus van handelingen in een informatiesysteem te beheersen, zodanig dat beschikbaarheid, integriteit of vertrouwelijkheid kan worden gecompromitteerd.

Taken rondom bedrijfsmiddelen (aanmaken van accounts), zijn uitbesteed aan onze ICT-leverancier. Hierin is scheiding aangebracht tussen degene die mutaties doorgeeft aan de ICT-leverancier en degene die controleert of deze mutaties juist en volledig zijn verwerkt. Om scheiding van taken te borgen maken wij binnen Optimo gebruik van workflows.

## Informatiebeveiliging in projectbeheer

Wij stemmen per opdracht af of er sprake is van afwijkende/ aanvullende maatregelen (boven op de standaard) die nodig zijn voor het uitvoeren van werkzaamheden voor de klant. Indien een klant een specifieke extra eis heeft dan kan dit worden vastgelegd in het dossier van de klant.

## Mobiele apparatuur en telewerken

Bij Optimo maken de medewerkers gebruik van een laptop en mobiele telefoon. Deze mobiele apparatuur wordt bij indiensttreding verstrekt, waarbij de medewerker moet tekenen voor het in ontvangst nemen van deze mobiele apparatuur. Bij het tekenen van de arbeidsovereenkomst gaat de medewerker akkoord met de arbeidsvoorwaarden (gedragsregels), aangaande het gebruik van deze bedrijfsmiddelen. Iedere laptop is voorzien van standaard geïnstalleerde software. Daarnaast zijn medewerkers vrij om zelf software te installeren indien zij dit voor hun werkzaamheden nodig hebben. Medewerkers kunnen hun werkzaamheden in principe verrichten op iedere locatie. Daarbij dienen zij beveiligingsmaatregelen, waaronder het maken van verbinding via een VPN, in acht te nemen. In de arbeidsvoorwaarden zijn ook bepalingen opgenomen ten aanzien van geheimhouding, bijvoorbeeld omtrent klantdata.

Binnen Optimo zijn meerdere medewerkers extern ingehuurd. Externe medewerkers die intern binnen Optimo actief zijn krijgen eveneens de beschikking over een laptop van Optimo. Voor hen gelden dezelfde gedragsregels als voor het eigen medewerkers.

Voor externe medewerkers die actief zijn op opdrachten voor klanten gelden dezelfde gedragsregels als voor eigen medewerkers. Door het tekenen van de inhuurovereenkomst conformeren externe medewerkers zich aan het informatiebeveiligings- en privacybeleid van Optimo.

## Veilig personeel

Voor Optimo zijn medewerkers een belangrijke factor als het gaat om informatiebeveiliging en privacy. Kennis en bewustzijn zijn essentieel voor informatiebeveiliging en privacy. De eisen op het gebied van informatiebeveiliging en privacy die aan de medewerkers worden gesteld gelden voor zowel interne medewerkers met vaste en tijdelijke aanstelling als voor externe medewerkers. De eisen worden bepaald door de rol, taak of functie van de medewerker.

Optimo heeft een aantal uitgangspunten om medewerkers betrokken en bewust te maken van informatiebeveiliging en privacy:

- Het MT is actief betrokken bij informatiebeveiliging en privacy en heeft daarmee een voorbeeldfunctie richting de medewerkers;
- Medewerkers worden periodiek geïnformeerd over informatiebeveiliging en privacy;
- Medewerkers worden betrokken bij de invulling van de maatregelen en interne audits voor informatiebeveiliging en privacy. Standaard onderdeel van het indiensttredingsproces is dat de medewerker een AVG-sessie krijgt van de FG, zodat de AVG-awareness wordt verhoogd
- Optimo hanteert vaste procedures bij in- en uitdiensttreding, waarin maatregelen op het gebied van informatiebeveiliging en privacy zijn opgenomen;
- Nieuwe medewerkers, zowel intern als extern, ondertekenen bij indiensttreding een geheimhoudingsverklaring;
- Optimo werkt planmatig aan de opbouw van kennis en bewustzijn op het gebied van informatiebeveiliging.

Bij het aannemen of inhuren van nieuwe medewerkers en het laten verrichten van werkzaamheden door externe medewerkers wordt bewerkstelligd dat zij hun verantwoordelijkheden begrijpen ten aanzien van informatiebeveiliging en privacy. Deze verantwoordelijkheden zijn vóór het dienstverband vastgelegd in een passende functiebeschrijving/opdracht en in de arbeidsovereenkomst/inhuurovereenkomst.

Bij indiensttreding overleggen alle medewerkers (intern en extern) een specifiek voor de functie verstrekte Verklaring Omtrent het Gedrag (VOG). Voor het gebruik van Optimo informatie gelden de rechten en plichten zoals vastgelegd in de diverse documenten, zoals de arbeidsvoorwaarden en geheimhoudingsverklaring. Het plegen van inbreuk op de informatiebeveiliging kan disciplinaire maatregelen tot gevolg hebben.

Bij uitdiensttreding wordt de vertrekkende medewerker gewezen op het na het dienstverband van kracht blijven (waaronder het relatie- en een geheimhoudingsbeding) van de arbeidsvoorwaarden.



## Beheer van bedrijfsmiddelen

### Inventariseren van bedrijfsmiddelen

Optimo heeft gedocumenteerd welke bedrijfsmiddelen worden gebruikt en hoe het eigenaarschap daarvan belegd is. Bedrijfsmiddelen die aan medewerkers van Optimo beschikbaar worden gesteld, dienen voor zakelijke doeleinden toegepast te worden en conform het informatiebeveiligings- en privacybeleid te worden gebruikt.

Opgeslagen en verwerkte informatie van of voor Optimo op bedrijfsmiddelen van Optimo blijft te allen tijde eigendom van Optimo. De privacywetgeving wordt gehandhaafd wanneer een beroep wordt gedaan op eigendomsrechten. Informatie is geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.

De bedrijfsmiddelen worden beheerd in overeenstemming met het binnen Optimo vastgestelde classificatieschema. Informatie op bedrijfsmiddelen wordt op een veilige manier verwijderd.

### Vertrouwelijkheidsclassificatie van informatie

Informatie wordt geclassificeerd om een passende mate van beveiliging van informatie te kunnen borgen. Niet alle informatie is even gevoelig en kritiek. Als geen classificatie is toegepast is informatie niet vertrouwelijk, tenzij uit de aard van de informatie blijkt dat deze als vertrouwelijk moet worden gezien. Optimo beschouwt onder andere persoonsgegevens, financiële gegevens en contracten als vertrouwelijk, ook als deze niet als zodanig zijn geclassificeerd.

### De Optimo Classificaties

Binnen Optimo wordt informatie geclassificeerd in de volgende klassen:

- Openbaar
- Intern gebruik
- Vertrouwelijk
- Geheim

Per classificatie gelden aparte voorschriften ten aanzien van opslaan, wijzigen, archiveren, vervoer, kopiëren, vernietigen, verspreiden, verzenden en herclassificeren.

## Toegangsbeveiliging

Toegang tot informatie en netwerken zullen op basis van 'need to know' worden beperkt zodat gebruikers toegang krijgen tot datgene wat noodzakelijk is voor het uitvoeren van de functie. De toegang wordt verstrekt aan de hand van de rol/functie. Toegang tot informatiesystemen wordt geïnitieerd door de manager van de medewerker op basis van het toekennen van een autorisatieprofiel die hoort bij de medewerkersrol. Jaarlijks worden de rollen en functieprofielen gecontroleerd aan de hand van de autorisatiematrix.

Het ontzeggen of wijzigingen van toegang tot informatiesystemen wordt eveneens geïnitieerd door de manager.

Na het afmelden van medewerkers of externe medewerkers die uit dienst zijn of waarvan de opdracht is gestopt, worden eveneens geïnitieerd door de manager.

Minimaal 1 week voor indiensttreding dient er een aanvraag gedaan te worden voor een nieuw account. Hierbij wordt er in de aanvraag op basis van de verstrekte informatie vanuit HR / recruitment een AD-account aangevraagd in het formaat [voornaam.achternaam@optimo.nl](mailto:voornaam.achternaam@optimo.nl). Dit account moet uniek zijn betreft de naam en dit wordt gecontroleerd door Xcellent. Naast het e-mailadres worden in het AD account de volgende zaken vastgelegd:

User logon name: [voornaam.achternaam@optimo.nl](mailto:voornaam.achternaam@optimo.nl)

First name: verplicht in dit voorbeeld voornaam

Initials: NIET VERPLICHT

Last name: verplicht in dit voorbeeld achternaam (zonder spaties)

Full name: verplicht

Email address: zelfde als username

Email alias: iets als tdbf of bijvoorbeeld rmi

Naast de hierboven genoemde richtlijnen voor het aanvragen van een AD account hanteren wij het standaard wachtwoorden beleid van Microsoft welke via policy's wordt afgedwongen. Zie voor meer informatie de [documentatie](#) van Microsoft.

## Wachtwoordbeleid

Optimo maakt gebruik van standaard group policy's die voor elke medewerker worden afgedwongen.

- Multifactorautorisatie (MFA)
- Dat er periodiek een verplichte wachtwoord wijziging gedaan moet worden aan de hand van de regels voor wachtwoorden welke Microsoft standaard afdwingt.
  - Bitlocker activatie (elke laptop wordt uitgereikt met een geactiveerde bitlocker)

## Cryptografie

Optimo zorgt voor correct en doeltreffend gebruik van cryptografie (versleutelen van informatie) om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.

Het gebruik van informatiesystemen, alsmede uitzonderingen en informatiebeveiligingsincidenten, worden vastgelegd in logbestanden op een manier die in overeenstemming is met het risico, en zodanig dat tenminste wordt voldaan aan alle relevante wettelijke eisen.

Cryptografische technieken worden toegepast voor:

Het beveiligen van harde schijven van laptops, zodat bij verlies of diefstal opgeslagen gegevens onbruikbaar zijn. Bij Optimo gebruiken wij hiervoor Bitlocker;

Transportbeveiliging van de websites (SSL) / https certificaten;

Beveiliging van VPN-verbindingen voor alle medewerkers;

Beveiliging van het Wifi netwerk, scheiding van gasten en bedrijfsnetwerk;

Beveiligde sFTP server welke enkel via SSH werkt.

Een wachtwoord management systeem waarin gevoelige informatie is opgeslagen (KeePass).

Cryptografische sleutels worden beheerd door de ICT-leverancier.

## Fysieke beveiliging en beveiliging van de omgeving

Optimo huurt een etage in een kantoorpand, waarin meerdere huurders aanwezig zijn. De toegang tot zowel de garage als het bovenliggend kantoorpand is beveiligd met toegangscontrole.

In het gehele kantoorpand is (ook buiten kantoortijden) beveiligingspersoneel aanwezig, welke toegang heeft tot het gehele gebouw. Zij zorgen op de daluren (voor 08:00 & na 18:00) voor de bemensing van de gezamenlijke receptie. Tijdens reguliere kantooruren is de receptie op de begane grond ook altijd bemand en bezoekers dienen zich te allen tijde te melden. Dit geldt zowel voor toegang tot het pand via de hoofdingang als bij het inrijden van de garage.

Optimo onderkent in het pand drie beveiligingszones:

De publieke zone die bestaat uit de centrale hal van het pand. Deze hal is voor iedereen toegankelijk. In de centrale hal bevindt zich een receptie waar bezoekers zich moeten melden.

De interne zone die alleen toegankelijk is voor medewerkers die in het bezit zijn van een toegangstag. Bezoekers mogen deze zone alleen betreden onder begeleiding van een gastheer of gastvrouw.

Extra beveiligde zone die alleen toegankelijk zijn voor medewerkers met speciale toegangsrechten.

Er wordt gebruik gemaakt van cameratoezicht voor alle toegangs- en vluchtdeuren.

## Clean desk en clear screen

Het clean desk en clear screen beleid staan beschreven in de arbeidsvoorwaarden (gedragsregels).

De kern van dit beleid:

- Medewerkers dienen hun laptop te vergrendelen als zij hun bureau (tijdelijk) verlaten. Wij spreken hier elkaar op aan;
- Bureaus dienen opgeruimd (leeg) te zijn, papieren worden opgeborgen in een afsluitbare lade of weggegooid in de daarvoor bestemde afsluitbare papiercontainers;

## Beveiliging bedrijfsvoering

Bedieningsprocedures worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben. Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging en privacy worden beheerd in de vorm van Wijzigingsbeheer. Informatie en informatieverwerkende faciliteiten worden beschermd tegen malware en technische kwetsbaarheden worden beheerd. Regelmatig worden back-up kopieën van informatie, software en systeemafbeeldingen gemaakt. Op deze manier wordt de continuïteit van de gegevensverwerkingen gegarandeerd. Gebeurtenissen worden d.m.v. logbestanden vastgelegd, bewijs verzameld en beoordeeld. Op basis van informatie in logbestanden wordt periodiek of naar aanleiding van een incident inhoudelijk getoetst op integriteit en vertrouwelijkheid

## Wijzigingsbeheer

Wijzigingsbeheer is volgens vastgestelde procedures ingericht.

## Back-up

Alle backup faciliteiten zijn extern belegd bij Xcellent en AFAS software. Ons interne bedrijfsnetwerk en informatie wordt volgens de SLA met Xcellent elke dag gebackuppeld en onze AFAS Profit omgeving door AFAS Software.

## Bescherming tegen malware

Optimo heeft virusscanners draaien die continu worden voorzien van de nieuwste virusdefinities. Het Optimo netwerk is beveiligd met firewalls. Bovendien is ons netwerk opgedeeld in meerdere segmenten. Ook tussen deze segmenten zorgen firewalls voor beveiliging tegen ongewenste toegang. Daarnaast wordt periodiek een securityscan uitgevoerd door de ICT-leverancier.

Door middel van awareness programma's worden medewerkers bewuster gemaakt in het herkennen van de verschillende vormen van malware en de risico's daarvan.

## Communicatiebeveiliging

Om informatie te beschermen worden netwerken via de ICT-leverancier beheerd en beheerst. Netwerken zijn gescheiden (groepen van informatiediensten, -gebruikers en -systemen). Het transporteren van informatie naar een externe partij vindt beveiligd plaats. Berichten worden beschermd tegen onbevoegde toegang, wijziging of weigering van dienstverlening in overeenstemming met het classificatieschema. Bij Optimo is er enkel communicatie mogelijk tussen een laptop en het intern bedrijfsnetwerk via een VPN verbinding via Direct Access.

## Informatietransport

Voor het delen van vertrouwelijke informatie met externen zijn voorzieningen getroffen om veilig informatietransport mogelijk te maken. De enige gebruikte methoden waarop informatie gedeeld mag worden zijn beschreven in het beleid “Uitwisseling data met derden”. De goedgekeurde methoden zijn:

- Via een sFTP server waarop de klant en Optimo medewerker toegang hebben.
- Via een klantportaal (via AFAS InSite / AFAS OutSite)
- Via een wachtwoord beveiligd ZIP bestand, waarbij het wachtwoord via verschillende kanalen wordt verstrekt.

## Acquisitie, ontwikkeling en onderhoud van informatiesystemen

Informatiebeveiliging maakt integraal deel uit van informatiesystemen in de gehele levenscyclus. De eisen die verband houden met informatiebeveiliging en privacy worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.

## Leveranciersrelaties

Optimo maakt gebruik van leveranciers voor het leveren van producten en diensten waarbij informatiebeveiliging en privacy een rol speelt. Bij deze producten en dienstverlening worden afspraken gemaakt over toegestane toegang tot bedrijfsmiddelen en de benodigde mate van informatie -beveiliging.

Bij de selectie van leveranciers wordt een standaard proces doorlopen, waarin de ze worden getoetst op onder andere technische en functionele geschiktheid, juridische aspecten, continuïteit en beveiligingsaspecten.

Met elke leverancier wordt afspraken gemaakt met betrekking tot geheimhouding.

Met alle leveranciers die persoonsgegevens verwerken wordt een (sub)verwerkersovereenkomst afgesloten.

## Beheer van beveiligingsincidenten

Optimo heeft het incident managementproces geïmplementeerd. Binnen dat proces kan een incident geclassificeerd worden als Informatiebeveiligings- of privacy incident. Deze typen incidenten worden afgehandeld door de Privacy Officer (FG) en/of Security Officer en besproken in het informatiebeveiligings- en privacy overleg (IBPO). Deze overlegstructuur is beschreven in het Optimo Management Systeem (OMS).

Het afhandelen van incidentmeldingen wordt gedaan conform die hiervoor opgestelde procesbeschrijvingen.

Optimo informeert haar klanten en medewerkers snel en zorgvuldig over verstoringen die de voor hen relevante diensten raken.

## Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

Optimo heeft procedures, rollen en verantwoordelijkheden bij het optreden van calamiteiten. Onder calamiteiten verstaan we onder andere ernstige verstoringen van de dienstverlening, uitval van faciliteiten en uitval van medewerkers. Optimo test jaarlijks haar continuïteitsplan. Aan de hand van de resultaten van deze test worden de plannen bijgesteld en wordt de organisatie bijgeschoold.

## Naleving

Optimo heeft inzicht in de toepasselijke wet- en regelgeving en contractuele verplichtingen betreffende klanten, leveranciers en samenwerkingspartners. Afspraken over intellectueel eigendom en privacyaspecten worden altijd contractueel vastgelegd.

Naleving van het informatiebeveiligings- en privacy beleid wordt periodiek getoetst. Bij oplevering van specifieke diensten vindt aanvullende toetsing plaats. Jaarlijks wordt een informatiebeveiligingsaudit uitgevoerd.

Voor informatie wordt de bewaartermijn, het opslagmedium en eventuele vernietiging bepaald in overeenstemming met wet, regelgeving, contractuele verplichtingen en bedrijfsmatige eisen.

Privacy en bescherming van persoonsgegevens is gewaarborgd in overeenstemming met relevante wet- en regelgeving en de verwerkersovereenkomsten met klanten en relaties. Ook conformeert Optimo zich aan de regelgeving omtrent de AVG (Algemene Verordening Gegevensbescherming).