otherside at work

for happy professionals

BEVEILIGINGSAANPAK

OTHERSIDE AT WORK

VERSIE	1.0
STATUS	Definitief
DATUM	12 maart 2018
CLASSIFICATIE	Openbaar

INHOUDSOPGAVE

INLEIDING

Otherside hecht zeer veel waarde aan de beveiliging van de gegevens van haar klanten, alsmede de privacy-rechten van betrokkenen waarover gegevens worden verzameld. De hoge eisen die wij hieraan stellen komen tot uiting in zowel fysieke, technische alsook procedurele maatregelen welke wij zowel intern als bij onze leveranciers voorschrijven, naleven en controleren.

De beveilingingsaanpak van Otherside wordt in deze brochure uitgesplitst naar de volgende onderwerpen:

1. Beveiliging:
    a. Inbedding informatiebeveiliging in de organisatie
    b. Logische en fysieke toegangsbeveiliging
    c. Functioneel beheer, verbindingen en hosting
    d. Monitoring en verbetering beveiligingsmaatregelen & -incidenten
    e. Softwareontwikkeling
    f. Back-up & restore procedures
2. Privacy:
    a. Verwerkersovereenkomsten
    b. Privacy officer
    c. Loket betrokkenen
    d. Bewaartermijnen
    e. Privacy-by-design

Deze brochure geeft u een indruk van de wijze waarop Otherside invulling geeft aan beveiliging. Voor verdere vragen kunt u vanzelfsprekend contact met ons opnemen.

Tevens willen wij u wijzen op het ISO-27001 certificaat, dat Otherside in oktober 2012 heeft behaald. Hiermee is het managementsysteem waarmee Otherside de risico's rondom de beschikbaarheid en beveiliging van Xpert Suite beheerd volgens deze internationale standaard geauditeerd, gecertificeerd en geaccrediteerd.

Daarnaast worden de controls van de annex A jaarlijks geaudit, waarna een ISAE3402 type II verklaring wordt afgegeven.

1 BEVEILIGING

1.1 Inbedding informatiebeveiliging in de organisatie

De informatiebeveiliging wordt beheerst via het ISO 27001 gecertificeerde Information Security Management Systeem (ISMS), geregistreerd via BSI Group onder certificaatnummer ISC-077. De beheerder hiervan is de 'security officer' die tevens directielid is. Het managementsysteem maakt integraal onderdeel uit van de (jaarlijkse) besturingscyclus van het bedrijf als geheel:

- Ieder jaar wordt een risico-analyse uitgevoerd op basis van de ervaringen van het afgelopen jaar en ontwikkelingen in de omgeving;
- Op basis van de risico-analyse worden verbeterplannen gemaakt die ter goedkeuring aan het directieteam worden overlegd;
- Na goedkeuring wordt uitvoering van deze verbeterpunten door het MT integraal in de sturing van het bedrijf bewaakt.

Naast het managementsysteem zijn er beheersprocessen ingericht waar afzonderlijke verantwoordelijken sturing op geven. Elk proces kent een eindverantwoordelijke die, in samenspraak met de directie, bepaalt wanneer en waarop controles plaatsvinden. Of elke verantwoordelijke ook daadwerkelijk zijn rol pakt wordt tenslotte gecontroleerd in de jaarlijkse interne en externe ISO-audit. De ingestelde controls/maatregelen, zoals benoemd in ISO 27002, zijn allen in beheer en worden gecontroleerd.

De volgende beheersprocessen zijn ingericht:

1. Asset & change management (incl. sleutelbeheer – Encryptie);
2. Patch management & Hardening;
3. Capaciteitsmanagement;
4. Toegangsmanagement;
5. Incidentmanagement;
6. Beheer derde partijen;
7. Personeelsmanagement;
8. Compliance management;
9. Continuïteitsmanagement;
10. Klantenmanagement.

Binnen het personeelsmanagement is expliciet aandacht voor:

- Awareness op het gebied van informatiebeveiliging; Er worden meerdere keren per jaar kennisavonden gehouden over het belang van informatiebeveiliging voor onze klanten en het voortbestaan van ons bedrijf. Tevens worden periodiek posters en andere visuele middelen gebruikt om mensen op procedures te wijzen. Voorbeelden hiervan zijn de lijsten die bij de papierbak en de printer hangen van welke spullen wel en welke niet hierin weggegooid dan wel geprint mogen worden. Ook in het personeelshandboek zijn diverse richtlijnen rondom informatiebeveiliging opgenomen en wordt actief gewezen op het informatiebeveiligingsbeleid. Bij het creëren van awareness op het gebied van informatiebeveiliging worden naast procedures ook potentiële grote gevolgen van verkeerd handelen getoond. Deze gevolgen hebben betrekking op de personen en klanten waarover informatie in onze systemen vastligt. Dit heeft als doel medewerkers niet alleen te motiveren om puur de procedures te volgen, maar ook om altijd zelf kritisch te blijven nadenken of er handelingen worden verricht die voor onze klanten en dus ook voor Otherside zelf grote nadelige gevolgen kunnen hebben.

- Competenties; Er wordt actief beoordeeld, bij indiensttreding en daarna elk jaar, of competenties van medewerkers aansluiten bij de functie die zij hebben of dat hier ontwikkeling in nodig is. Wanneer competenties niet meer aansluiten bij de functie, is een wijziging van functie een mogelijkheid. Bij personele wijzigingen wordt actief beoordeeld of de juiste competenties nog in het bedrijf aanwezig zijn of dat er gaten ontstaan. Wanneer het laatste het geval is, wordt gekeken hoe deze competenties binnen de organisatie opnieuw te ontwikkelen dan wel binnen te halen.

- Integriteit; Bij de aanname van medewerkers worden een aantal acties uitgevoerd om vast te stellen of de persoon integer is voor het werken met privacygevoelige gegevens:
    - Diploma/referentiecheck;
    - VOG aanvragen;
    - Ondertekenen geheimhoudingsverklaring;
    - Klant specifieke screenings.

- Actieve beoordeling op werken in lijn met informatiebeveiligingsbeleid; In hoeverre een medewerker handelt naar het informatiebeveiligingsbeleid is onderdeel van het beoordelingsgesprek. Indien een medewerker hier niet goed op acteert, worden actief waarschuwingen gegeven die kunnen resulteren in beëindiging van de dienstbetrekking. Het zelf melden van zelf veroorzaakte incidenten wordt veel minder negatief beoordeeld, dan dat een andere medewerker een melding doet. Dit om te voorkomen dat er een angstcultuur ontstaat.

1.2 Logische en fysieke toegangsbeveiliging

Belangrijkste maatregel is de strikt fysieke en logische scheiding van de kantoor-omgeving (zonder klantgegevens m.u.v. financiële administratie) en de productie-omgeving (met klantgegevens). Hiervoor geldt:

1. Geen enkele medewerker van Otherside heeft fysiek zelfstandig toegang tot de ruimtes waar klantgegevens zijn opgeslagen. Hiervoor is altijd medewerking van de hostingpartner (Proserve) noodzakelijk en goedkeuring van de directie.
2. Medewerkers van Proserve kunnen fysiek bij de apparatuur waar klantgegevens zijn opgeslagen. Deze gegevens zijn echter opgeslagen op geëncrypte schijven en in geëncrypte databases, waardoor voor medewerkers van Proserve de klantgegevens niet leesbaar zijn.
3. De fysieke toegang tot de kantooromgeving wordt door de facility manager vastgelegd in een sleutelplan en jaarlijks door de directie beoordeeld. De ruimtes die in dit sleutelplan worden behandeld zijn: werkplekken (algemeen), werkplek financiële administratie, serverruimte kantooromgeving (geen klantgegevens) en archief met administratie.
4. De logische toegang tot de kantooromgeving wordt door werkplekbeheer operationeel beheerd. Ook hiervoor geldt dat de uitdraai van de active directory en toegangsrechten op de verschillende servers jaarlijks wordt gecontroleerd door de directie.
5. In het indiensttredings- en uitdiensttredingsprotocol is een checklist opgenomen waarmee wordt gecontroleerd of alle fysieke en logische toegang is afgesloten. Daarnaast zijn in de checklist een aantal andere stappen opgenomen aangaande het inleveren van apparatuur en aanverwante zaken.
6. De logische toegang tot de productie-omgeving is apart afgeschermd:
    a. Er is voor een beperkte set medewerkers toegang tot de productie-omgeving. Dit uitsluitend indien noodzakelijk voor de uitoefening van eigen functie.
    b. Medewerkers met toegang krijgen een aparte gebruikersnaam en wachtwoord, geïnstalleerd certificaat en een tweede factor (time-based token) om in te loggen op de productie-omgeving. Inloggen gaat doormiddel van een VPN-verbinding, wat alleen mogelijk is vanaf de IP-range van kantoor Otherside dan wel een backup-locatie.
    c. Toegang voor geautoriseerde medewerkers tot de servers is beperkt op basis van functie. Alleen de voor de eigen functie noodzakelijke servers zijn toegankelijk.
    d. Toegangsrechten worden actief bijgewerkt bij functiewijzigingen en uitdiensttreding. De verstrekte rechten worden jaarlijks door de directie gecontroleerd op juistheid.
    e. Toegang tot productie-databases via de webinterface zijn, net zoals voor alle andere gebruikers, altijd beveiligd met 2-factor-authenticatie.

Het beheer van fysieke en logische toegang is ondergebracht in de toegangsmanagementprocedure die eveneens onderdeel is van het ISO27001:2013 gecertificeerde ISMS.

1.3 Functioneel beheer, Verbindingen en hosting

Binnen de Xpert Suite kunnen klantbeheerders zelf rollen definiëren en toekennen aan gebruikers. Op basis van deze rollen wordt door de software bepaald welke wijzigingen gebruikers wel, en welke zij niet mogen doorvoeren. Basis van

deze autorisatie is dat de rol bepaalt wat een gebruiker mag doen en dat de koppeling aan medewerkersdossiers van de individuele gebruiker bepaalt voor wie dat mag. Tezamen bepalen deze autorisaties of een wijziging wel of niet wordt toegestaan. Hierbij geldt uiteraard dat alle binnenkomende wijzigingen door de server op de ingerichte autorisaties worden beoordeeld. Beheerders kunnen een IST-matrix van de wat autorisaties en alle ingerichte rollen uitdraaien om deze intern te laten toetsen (IST vs SOLL).

Voor het beheer van de servers, waarop de software en klantgegevens staan, geldt dat een medewerker ook een in de Active Directory gedefinieerde rol toegewezen krijgt. Deze rol-toewijzing wordt bijgehouden en periodiek gecontroleerd op juistheid. Vervolgens wordt het standaard windows-mechanisme gebruikt voor beperking van rechten. Voor toegang tot de beheeromgeving moet een VPN-verbinding worden gelegd die een IP-filtering en een 2-factor-authenticatie kent. Toegang is daarnaast uitsluitend mogelijk vanaf de IP-range van kantoor Otherside dan wel een backup-locatie.

Als aanvullende maatregel heeft Otherside een SIEM ingericht die zowel het dataverkeer als de logging van uitgevoerde acties verzamelt en analyseert. Hiermee kan aanvullend worden beoordeeld en actief worden geëscaleerd indien een gebruiker of softwarecomponent 'ongewone' acties verricht.

Al het verkeer naar de productie-omgeving komt via een fysieke firewall binnen, waarbij alleen verkeer wordt toegestaan wat expliciet wordt opengezet en dus is goedgekeurd via de change-procedures. Vervolgens wordt het verkeer gerouteerd over een gesegmenteerd netwerk, waarbij alleen de web- en koppeling servers die daarvoor bedoeld zijn bereikbaar zijn via internet.

Webverkeer is altijd beveiligd via SSL, waarbij de SSL-instellingen via externe tools getoetst worden op bekende kwetsbaarheden. Bestandsuitwisselingen verlopen via VPN of SFTP.

De databaseservers zijn niet rechtstreeks te benaderen en de databases zijn per klant gescheiden. Opgeslagen data wordt middels het TDE-mechanisme van SQL Server geëncrypt én er vindt daarnaast cell-level encryptie plaats voor medische gegevens die door bedrijfsartsen worden ingevoerd. De cell-level encryptie vindt plaats via de applicatie met een klant- en applicatiesleutel.

De data is opgeslagen in de volgende primaire locatie:
EU Networks
Paul van Vlissingenstraat 16
1096 BK Amsterdam

De backups en disaster-recovery staat op de volgende locatie:
Dataplace
Van Coulsterweg 6
2952 Alblasserdam

1.4 Audits en monitoring van verbetering Beveiligingsmaatregelen & -incidenten

Non-conformiteiten kunnen op een aantal manieren worden vastgesteld:

1. Tijdens de jaarlijkse interne audit;
2. Tijdens de jaarlijkse externe certificeringsaudit;
3. Tijdens de jaarlijkse ISAE3402 type II audit;
4. Als gevolg van de analyse van een gemeld incident.

Incidenten kunnen worden gemeld door klanten of medewerkers of het gevolg zijn van een (periodieke) controle van een beheersmaatregel door een verantwoordelijke contactpersoon.

Na het vaststellen van een non-conformiteit wordt een plan van aanpak opgesteld. Dit plan van aanpak richt zich op de vraag welke maatregelen noodzakelijk zijn de vastgestelde non-conformiteit op te heffen en te voorkomen dat deze herhaaldelijk optreedt. Een conclusie hierin kan bijvoorbeeld zijn dat ingerichte werkwijzen dusdanig suboptimaal zijn, dat de verleiding om deze te omzeilen te groot is en aanpassingen nodig zijn.

Om te monitoren of genomen maatregelen het gewenste effect hebben, wordt bij elke maatregel expliciet vastgesteld op welke manier en hoe vaak de effectiviteit wordt gemeten. De verantwoordelijke contactpersonen voeren de vastgestelde maatregelen vervolgens uit. Tijdens de audit wordt voor alle controls gecontroleerd of dit wel is gedaan.

Beveiligingsincidenten worden in periodieke awareness-sessies en, indien door een individu dan wel afdeling veroorzaakt, met de betrokken medewerkers besproken. Indien een beveiligingsincident leidt tot een (potentieel) datalek wordt de procedure 'Meldplicht Datalekken' gevolgd. Binnen deze procedure dienen verantwoordelijken binnen 24 uur te worden geïnformeerd conform de richtlijnen van de Autoriteit Persoonsgegevens.

De audits worden een aantal keer per jaar uitgevoerd:

- Eénmaal per jaar een interne audit, waarbij medewerkers van Otherside at Work controles op procedures uitvoeren van verantwoordelijken binnen de organisatie. Resultaten worden intern besproken en verbeteracties geïdentificeerd.
- Eénmaal per jaar een externe ISO 27001 certificeringsaudit (eens per 3 jaar een officiële certificering en daar tussen elk jaar een controle-audit). Op basis van deze audits wordt een verslag opgesteld en bepaald of Otherside at Work het certificaat mag behouden.
- Eén maal per jaar een ISAE3402 type II audit door een externe gecertificeerde auditor. Deze geeft een ondertekende verklaring van de uitgevoerde controles en gevolgen voor klanten.

1.5 Softwareontwikkeling

Otherside heeft Secure Development principes in haar ontwikkelmethodiek opgenomen. Bij elke individuele wijziging wordt, conform de eisen in de ISO 27001 richtlijnen, beoordeeld wat de impact op het gebied van beveiliging is. Ontwikkelaars maken hierbij gebruik van een checklist die is opgesteld op basis van de OWASP-top 10 richtlijnen, ISO27002 controls, NCSC en NIST. Bij elke release wordt aan de hand van deze checklist de gewijzigde code gereviewd en opgeleverd aan de afdeling Maintenance & Support. Vervolgens voert Maintenance & Support een aantal technische en functionele acceptatietests uit, waarbij de werking van autorisaties wordt getoetst voordat de release in productie wordt genomen.

Minstens éénmaal per jaar wordt een externe partij gevraagd om PEN-testen uit te voeren op de software. Hierbij wordt elke 2 jaar gewijzigd van PEN-test leverancier om een kritische analyse te waarborgen. Voor 2016 en 2017 worden deze tests uitgevoerd door Deloitte.

Secure programming competenties van ontwikkelaars worden met behulp van internen en externen ontwikkeld en up-to-date gehouden.

1.6 Back-up & restore procedures

Data wordt tegen vernietiging beschermd middels een backup proces dat de afgelopen 7 dagen, 3 weken (voor die 7 dagen) en 11 maanden (voor die 2 weken) wordt uitgevoerd op klantdatabases (effectief dus tot maximaal 12 maanden terug). De back-ups worden geëncrypt en periodiek getoetst door middel van restores. Doordat er losse back-ups per klant zijn, is restoren per klant mogelijk. Otherside kan mede hierdoor eenvoudig garanderen dat, indien dit gewenst is, alle data van een specifieke klant kan worden vernietigd.

Otherside heeft een permanente back-up locatie ingericht. Mocht de primaire locatie vernietigd worden, dan kan de applicatie weer up-and-running worden gebracht binnen de in de SLA afgesproken periode.

2 PRIVACY

In de Xpert Suite worden bijzondere persoonsgegevens verwerkt. Dit betekent dat de gevolgen voor betrokkenen erg groot kunnen zijn, mochten er fouten in de verwerking gemaakt worden. Uiteindelijk zijn de klanten van Otherside de verantwoordelijken voor deze verwerking, maar Otherside wil met haar procedures en maatregelen een platform bieden waarop de verantwoordelijke optimaal c.f. wettelijke eisen en rechten van betrokkenen de gegevens kan verwerken. Hierbij zullen we onze klanten waar mogelijk zo veel mogelijk sturen richting een compliant werkwijze.
Hieronder staan de extra maatregelen in het kader van privacy-wetgeving die Otherside heeft genomen.

2.1 Verwerkersovereenkomst

Otherside sluit met alle klanten die gebruik maken van haar software een verwerkersovereenkomst. Deze overeenkomst is getoetst om compliancy met de relevante privacy-wetgeving (in ieder geval de AVG). Een standaardverwerkersovereenkomst is op te vragen bij Otherside.

2.2 Privacy officer

Otherside heeft een privacy-officer en privacy- en security team samengesteld. Dit team bestaat uit alle vertegenwoordigers van alle onderdelen van de organisatie die potentieel in aanraking komen met klantgegevens (consultants, support, IT-management). In dit overleg worden alle lopende verbeteracties, incidenten en risico-analyses besproken, zodat er integrale bewaking op de beveiliging is.
De privacy officer is aangesteld om in dit overleg de impact van verbeteracties, incidenten en risico-analyses aan te vullen met gevolgen voor betrokkenen.

De privacy officer is:
Roel van der Sanden
roel.vandersanden@othersideatwork.nl
06-13874641

2.3 Loket betrokkenen

Otherside heeft voor de betrokkenen een loket ingericht waar ze met hun vragen terecht kunnen. In de basis geldt dat een verantwoordelijke (dus de klant van Otherside) de betrokkenen te woord moet staan. Maar blijkt dit niet mogelijk dan wil Otherside voor betrokkenen wel bereikbaar zijn en ondersteunen waar mogelijk in het oplossen van eventuele problemen.

Het loket is te bereiken op:
073-6159950
loket.betrokkenen@othersideatwork.nl

De informatie over het loket is ook opgenomen op de website van Otherside inzichtelijk.

2.4 Bewaartermijnen

Voor de vastgelegde gegevens in de Xpert Suite gelden erg verschillende bewaartermijnen (een werkgever moet een verzuimdossier binnen 2 jaar na uitdienst verwijderen, een arbodienst moet hem soms wel 40 jaar bewaren). Otherside heeft in haar software functionaliteit toegevoegd waarmee kan worden vastgelegd welke termijnen gehanteerd moet worden in welke situatie. Vervolgens geldt dat deze data nog 12 maanden in de oude versies van backups aanwezig kan zijn. Daarna is de data definitief verwijderd / vernietigd.

Deze backuptermijn is door langlopende dossiers van deze omvang. Soms komen gebruikers pas erg laat achter ten onrechte verwijderde gegevens. Rechten van betrokkenen betreffen ook de bewaarplicht. Omdat backups niet operationeel inzichtelijk zijn, hanteert Otherside deze termijn in afweging tussen aan de ene kant het recht op datavernietiging en aan de andere kant het recht van bewaarplicht.

2.5 Privacy-by-design en privacy-by-default

In het ontwerpproces van de software hanteert Otherside de volgende beginselen:

- Bij het maken van een ontwerp worden compliancy met privacy-wetgeving en gevolgen voor betrokkenen altijd in de analyse meegenomen
- Als een gebruiker geen keuze heeft gemaakt voor een setting, dan gaan we van de striktste privacy-instellingen uit (privacy-by-default)
- Als gebruikers van wettelijke verplichtingen lijken af te wijken, dan moeten ze hier altijd een reden voor opgeven (b.v. inloggen zonder 2FA)
- Op alle punten waar de software gebruikers kan ondersteunen in het privacy-compliant werken zal Otherside proberen zo gebruikersvriendelijk mogelijke oplossing inrichten, zodat gebruikers zo veel mogelijk deze compliant-werkwijze volgen (b.v. niet alleen SMS als 2FA, de Datakluis, DialoogXpert)
- De software ondersteunt het vastleggen van wettelijke grondslagen voor verwerking, ten behoeve van ondersteuning van verantwoordelijke.

Uiteraard kan Otherside niet garanderen dat elke gebruiker in de Xpert Suite compliant werkt met geldende wet- en regelgeving. Het aantonen hiervan blijft liggen bij verantwoordelijke.