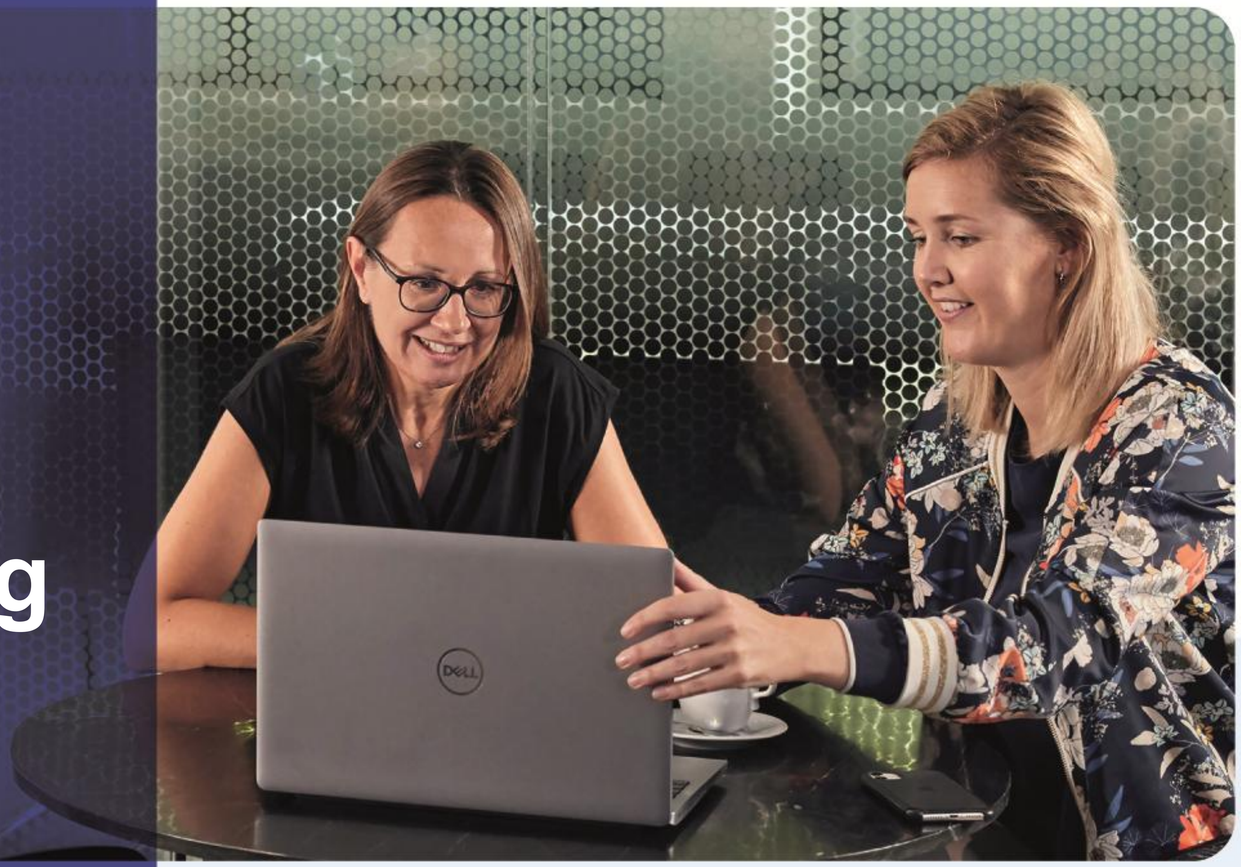
Zorg voor data

Toelichting Informatiebeveiliging SARI-registratie



21 augustus 2025 - versie 1.1

Vertrouwelijkheid: intern

Over dit document

Beste lezer,

Deze Toelichting Informatiebeveiliging is opgesteld om opdrachtgevers, klanten en leveranciers te informeren over welke maatregelen DHD heeft genomen om de SARI-registratie en de gegevens die DHD hiervoor worden verwerkt te beveiligen.

Mocht u vragen hebben voor bijvoorbeeld een (D)PIA of andere doeleinden, dan zult u een groot deel van alle informatie vinden in dit document.

Heeft u aanvullende (juridische) vragen? Dan kunt u contact opnemen met onze security officer, functionaris gegevensbescherming (FG) of jurist en privacy officer. Deze contactgegevens vindt u hiernaast.

Contactgegevens

DHD
Oudlaan 4
3515 GA Utrecht
info@dhd.nl

Security officer
Robert Kerssies
r.kerssies@dhd.nl

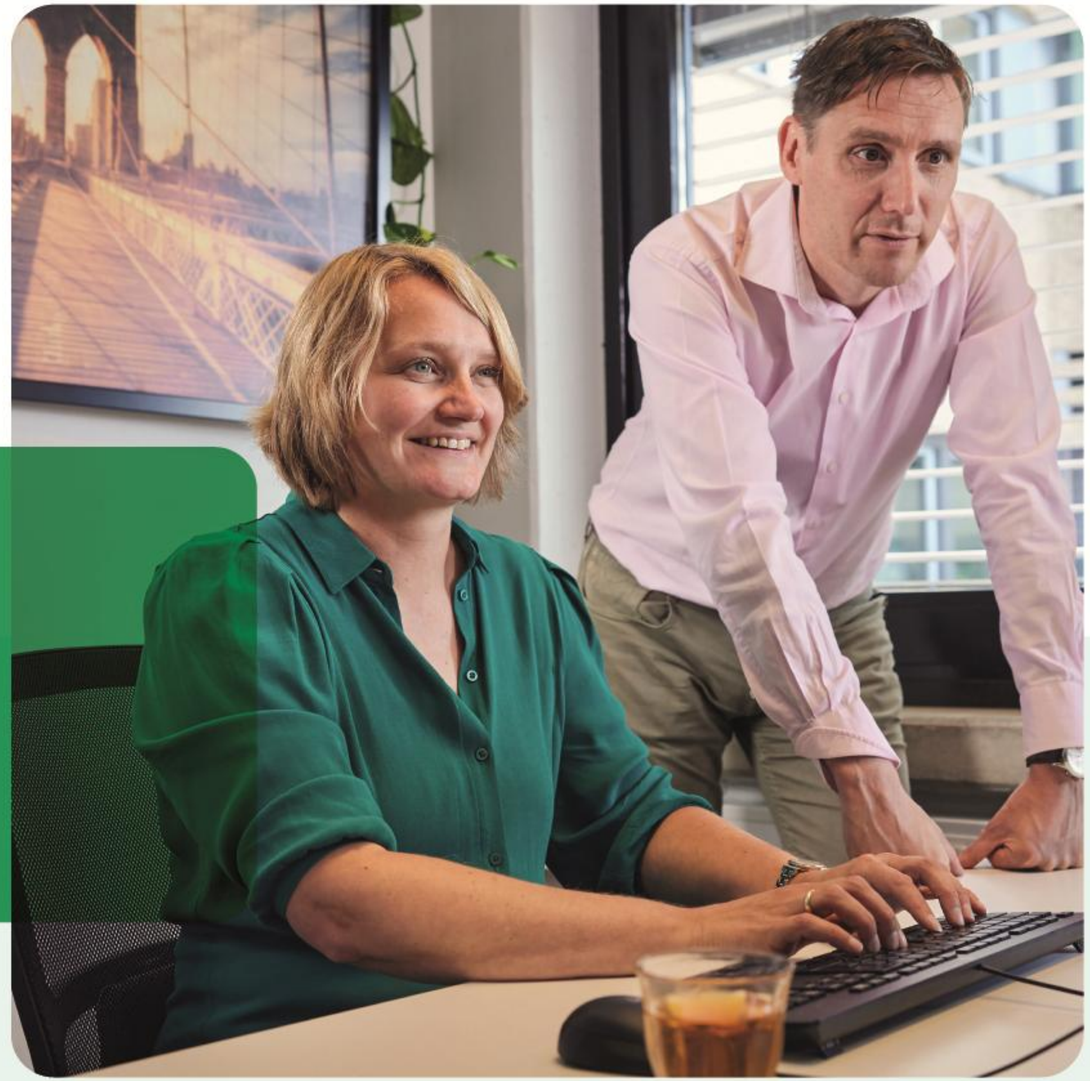
FG
Klaas-Wouter Geleynse
geleynse@dhd.nl

Jurist en privacy officer
Clemens van den Enden
c.vandenenden@dhd.nl

DHD Zorg voor data

Zorg voor data

Over DHD



Over DHD

Wij zijn DHD. Een team van gedreven experts die dagelijks in verbinding staan met alle ziekenhuizen en umc's. DHD is een stichting zonder winstoogmerk. Wij zijn in 2008 opgericht door de NVZ en NFU. Beide brancheorganisaties maken deel uit van het bestuur van DHD. In oktober 2022 is ook de Federatie Medisch Specialisten toegetreden tot het bestuur van DHD.

Wij stroomlijnen de samenwerking in de medisch-specialistische zorg op het gebied van data. Dit doen we door landelijke registratie-, data- en informatieprocessen te organiseren, projecten te coördineren, producten en diensten te ontwikkelen, kennis en expertise te leveren, onderzoek te faciliteren en ziekenhuizen met elkaar in contact te brengen. Zo hebben zorgprofessionals eenvoudig toegang tot zorg- en stuurinformatie en worden de administratieve lasten verlaagd.

De omgang met data brengt complexe vraagstukken met zich mee. Vastleggen, ontsluiten, valideren, analyseren, doorleveren, rapporteren, onderzoeken, duiden: hoe doe je dat zo efficiënt en veilig mogelijk?

Het antwoord ligt in **samenwerking**.

Speerpunten

- Slim registreren
- Efficiënt ontsluiten
- Leren van informatie
- Leren van elkaar
- Service verlenen

Certificeringen

DHD is in het bezit van de volgende certificaten. Voor vragen die verwijzen naar een norm uit bijvoorbeeld de ISO27001 of NEN7510/12, verwijzen wij naar de Verklaring van Toepasselijkheid. Deze kan op verzoek met u worden gedeeld.

DHD Zorg voor data

Zorg voor data

Gegevens-verwerking

Gegevensverwerking

Type gegevens
DHD verwerkt vanuit de SARI-registratie persoonlijke gezondheidsinformatie en medische patiëntgegevens.

Ophalen gegevens
De gegevens worden door de ziekenhuizen via de beveiligde Datahub van DHD aangeleverd. DHD heeft hierdoor toegang tot de volgende gegevens; geboortejaar en -maand, postcode, geslacht, patiëntnummer en diagnose-, laboratorium- en opnamegegevens.

Opgave gegevens
Wanneer er door een ziekenhuis wordt gevraagd om een opgave over welke persoonsgegevens DHD voor hen verwerkt van een bepaald individu, zal DHD deze binnen 5 werkdagen beschikbaar stellen. Dit kan via de functionaris gegevensbescherming.

Wijzigen gegevens
DHD beschikt over een interne procedure om persoonsgegevens van een bepaald individu op verzoek te verwijderen, corrigeren, afschermen of porteren. Dit kan via de functionaris gegevensbescherming.

Locatie
Alle persoonsgegevens worden verwerkt binnen de EU.

Cookies
DHD zal voor haar informatieproducten enkel functioneel noodzakelijke cookies gebruiken.

Eigendom gegevens
Alle persoonsgegevens zijn en blijven eigendom van de verwerkingsverantwoordelijke partij.

Wijzigen en vernietigen gegevens
Persoonsgegevens worden op verzoek binnen 5 werkdagen gewijzigd of verwijderd zodat deze juist en up-to-date zijn.

(IT) Onderaannemers
Met alle (IT) Onderaannemers heeft DHD overeenkomsten gesloten die de zorgvuldige verwerking van persoonsgegevens waarborgen. Deze voorziet in dezelfde plichten die wij aan onszelf opleggen. DHD werkt uitsluitend met (IT) Onderaannemers die de data verwerken binnen de EU.

Verwerkersovereenkomsten
DHD is bereid om met klanten een (sub)verwerkersovereenkomst af te sluiten.

DHD Zorg voor data

Doorlevering van SARI-gegevens

Aanleiding
Vanuit het RIVM is een gegevensverzoek afgegeven voor de surveillance van acute respiratoire infectieziekten. De ziekenhuizen geven DHD opdracht om deze SARI-gegevens te verstrekken aan het RIVM d.m.v. de dienstverleningsovereenkomst (DVO).

Doorlevering SARI-gegevens
De door de ziekenhuizen bij DHD aangeleverde SARI-gegevens worden voor de doorlevering aan het RIVM geanonimiseerd. De gegevens zijn hierdoor niet herleidbaar naar de patiënt of het ziekenhuis.

De gegevens worden via een secure SFTP-verbinding door geleverd naar het RIVM.

Type gegevens
Het RIVM heeft door de doorlevering zicht op het geslacht, de veiligheidsregio waarin de patiënt woonachtig is en de leeftijd. Voor kinderen jonger dan 2 jaar wordt de leeftijd weergegeven in maanden. Alle patiënten ouder dan 95 worden weergegeven als 95.

Indien er te weinig data aanwezig is om de veiligheidsregio geanonimiseerd weer te geven wordt deze omgezet naar een landelijke indicatie.

DHD Zorg voor data

Zorg voor data

Beleid en maatregelen

Beleid en maatregelen

Screening en geheimhoudingsverklaring
Alle medewerkers, zowel intern als extern, worden tijdens het sollicitatieproces gescreend d.m.v. een VOG, referentiecheck en socialmedia-check. Ook tekenen zij een geheimhoudings-verklaring.

Onboarding
Alle nieuwe medewerkers volgen een onboardingsprogramma. Daarnaast vindt er een kennisniveau-interview plaats en ontvangen zij het personeelshandboek. Ook krijgen zij instructies over o.a. het veilig inloggen op de verschillende omgevingen. Periodiek krijgen de medewerkers bijscholing over het informatiebeveiligingsbeleid en de procedures.

Wachtwoordbeleid
Alle medewerkers hebben de mogelijkheid om passwordless in te loggen via Windows Hello en de Microsoft Authenticator App. Alle medewerkers krijgen een unieke gebruikersnaam. Gedeelde accounts zijn niet toegestaan.

DHD volgt het wachtwoordbeleid wat door Microsoft wordt afgedwongen via Entra ID, voorheen Azure AD.

Clean Desk Policy
De medewerker dient zijn beeldscherm te vergrendelen wanneer hij of zij de werkplek verlaat. Na 10 minuten inactiviteit gebeurt dit automatisch. Medewerkers dienen zich te realiseren wie er met hun kan meekijken wanneer zij werken met vertrouwelijke informatie. Dit geldt ook voor papier op de bureaus en informatie op bijvoorbeeld whiteboards en tv-schermen.

Toegangsbeveiliging en bezoekers
Alle medewerkers hebben een toegangspas waarmee zij de afgesloten ruimtes kunnen betreden. Bezoekers dienen te allen tijde aangemeld te worden. Zij worden bij de receptie opgehaald door de contactpersoon en mogen zonder begeleiding de afgesloten ruimtes niet betreden.

USB-sticks
Het is verboden om gebruik te maken van USB-sticks of andere datadragers om data te transporteren.

Beleid en maatregelen

Devices
Alle apparaten die verbinding maken met de omgeving(en) van DHD dienen te voorzien te zijn van up-to-date antivirus software, beeldschermvergrendeling en een passend wachtwoord of pincode. In geval van twijfel mag deze apparatuur niet worden gebruikt.

Opslaan van data
(Strikt) Vertrouwelijke informatie mag enkel opgeslagen worden in een afgeschermde (online) omgeving. Het lokaal opslaan van vertrouwelijke informatie is niet toegestaan.

Softwaregebruik
Het is niet mogelijk voor de medewerker om software te installeren op de apparatuur van DHD. Voor privé-apparatuur is er een lijst beschikbaar met geschikte software. Wanneer extra software noodzakelijk is, loopt dit via de manager IT. Alle software dient voorzien te zijn van een geldige licentie.

Rechten
De medewerker krijgt enkel rechten wanneer hier door een teammanager toestemming voor is gegeven. De rechten worden maandelijks gecontroleerd op juistheid. Bij het uitdiensttreden worden de rechten direct ontnomen.

Beheerdersaccounts
Voor het uitvoeren van beheerwerkzaamheden dient de medewerker in te loggen met een priviliged account. De wachtwoorden van de beheeraccounts dienen minimaal 32 tekens lang te zijn en worden voorzien van MFA. Deze accounts worden beperkt toegekend.

Passwordmanager
Alle gebruikersnamen en wachtwoorden dienen veilig opgeslagen te worden. Hiervoor is er een passwordmanager beschikbaar gesteld aan alle medewerkers. Deze passwordmanager is niet verbonden aan het internet en heeft een lokaal geëncrypte database.

DHD Zorg voor data

Beleid en maatregelen

Externe accounts
Om klanten toegang te verlenen tot de producten van DHD, wordt er gebruik gemaakt van externe accounts. Gebruikersnaam en wachtwoord worden los van elkaar gedeeld (e-mail, telefonisch en SMS). Daarnaast worden er geen wachtwoorden opgeslagen of gedeeld, enkel met de eigenaar van het account.

Data vernietiging
Wanneer apparatuur niet meer wordt gebruikt wordt alle mogelijke data verwijderd en wordt de datadrager professioneel vernietigd. DHD ontvangt hiervan een certificaat.

Printen en papier
Printen gebeurt enkel via een uitgestelde of beveiligde printopdracht óf dient direct bij de printer afgehaald te worden. Papier blijft niet onbeheerd bij de printer liggen en wordt opgeborgen in een afsluitbare kast. Oud papier wordt gedeponeerd in de daarvoor bestemde (afgesloten) papierbak, afhankelijk van de classificatie van vertrouwelijkheid.

BYOD
Het is voor de medewerker toegestaan om gebruik te maken van eigen apparatuur. Hiervoor stelt DHD twee belangrijke eisen:

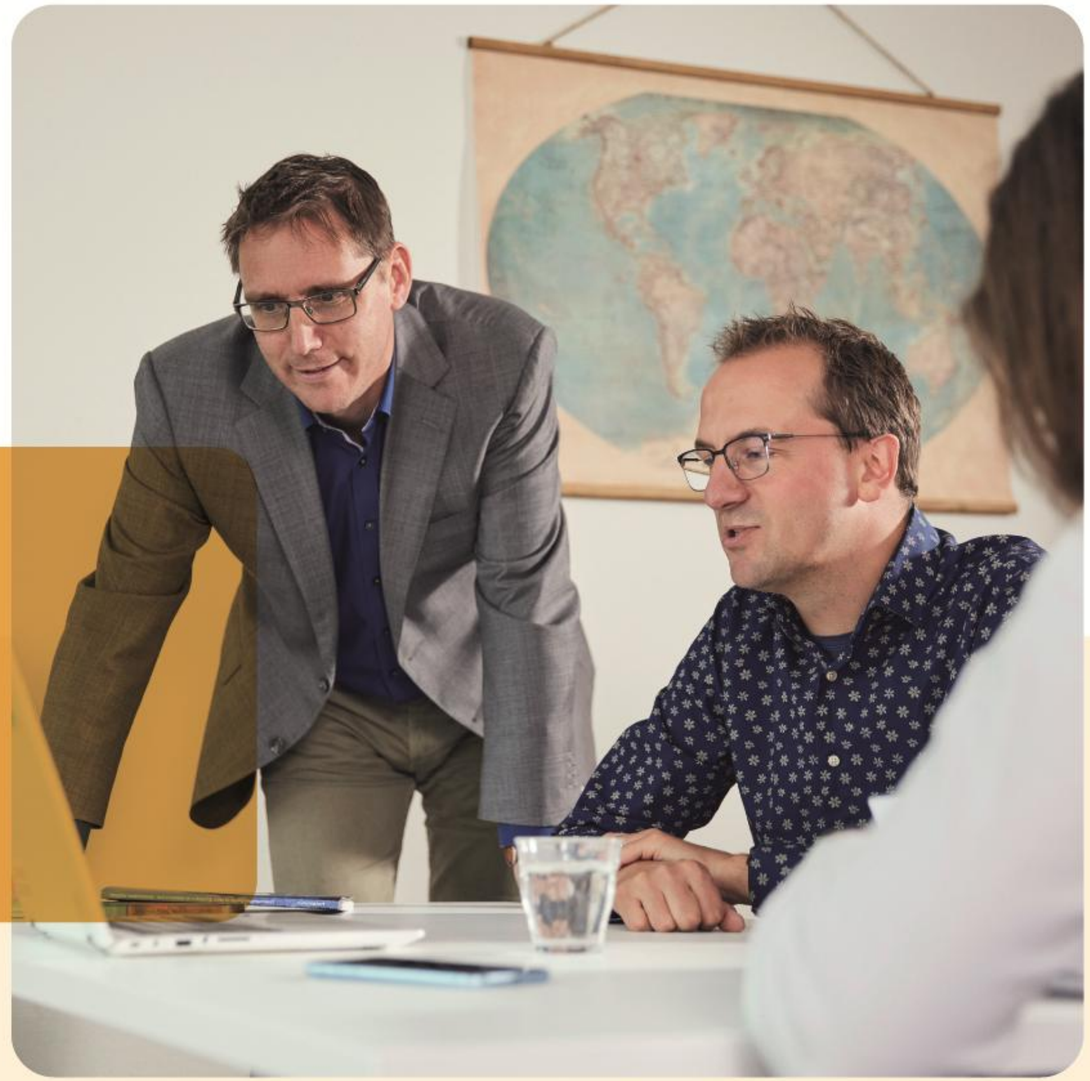
1. Het apparaat is voorzien van de laatste security updates
2. De disk van het apparaat is geëncrypt d.m.v. Bitlocker

Alle (privé)apparatuur wordt gemonitord via Microsoft Intune. Wanneer de medewerker hier niet mee instemt óf het apparaat hier niet aan kan voldoen, mag deze niet gebruikt worden voor de toegang tot de omgevingen van DHD.

DHD Zorg voor data

Zorg voor data

Technische maatregelen



Technische maatregelen

Security stack
Alle devices van DHD zijn voorzien van de security stack van Microsoft. Hierdoor worden mogelijke aanvallen door ransom- of cryptoware direct gedetecteerd en onderschept. Deze oplossing bevat ook Intrusion Detection & Prevention.

SIEM
Alle incidenten, kwetsbaarheden, (verdachte) gedragingen van gebruikers en beheerders worden real-time gemonitord en alle events hiervan worden geregistreerd in het SIEM (Microsoft Sentinel). Door hier lering uit te trekken en proactief op te acteren kan DHD de informatiebeveiliging continu verbeteren. Rapportages en logging worden dagelijks en wekelijks gecontroleerd.

Inloggen
Om toegang te krijgen tot de verschillende lagen van beschikbare informatie of rechten, dient de medewerker telkens per laag in te loggen met een separate gebruikersnaam en wachtwoord en MFA. Gebruikers- en beheerdersaccounts zijn van elkaar gescheiden. Hiervoor wordt gebruik gemaakt van Privileged Identity Management welke gemonitord wordt op verdachte gedraginge.

Logging en controle
Goedgekeurde en geweigerde inlogpogingen worden gelogd. Hierbij zijn aantallen, datum en tijdstip van niet goedgekeurde inlogpogingen, toegang tot bestanden/informatie buiten normale gebruikerstijden, significante gebruikershandelingen en aangetroffen malware en storingen onderdeel van de kwartaalrapportage.

De logging wordt 90 dagen bewaard. Logbestanden zijn uitsluitend beschikbaar voor een beperkt aantal aangewezen personen om onbevoegde toegang en vervalsing te voorkomen. In specifieke gevallen kan de bewaartermijn oplopen tot 24 (gebruikersstatistieken) of 60 maanden (incidenten).

In het geval van een (mogelijk) beveiligingsincident kan er worden afgeweken van de maximale bewaartermijn.

De activiteiten van alle (beheerders)accounts worden gemonitord en vastgelegd. Deze gegevens worden periodiek geanalyseerd.

Voor de logbestanden wordt gebruik gemaakt van één referentietijdbron (UTC) om de nauwkeurigheid te waarborgen.

DHD Zorg voor data

Technische maatregelen

SSO en MFA
Alle mogelijke applicaties zijn gekoppeld aan het Azure AD van DHD. Hierdoor wordt er waar het kan ingelogd via SSO. Bij het inloggen dient de medewerker zijn of haar identiteit te bevestigen d.m.v. MFA via de Microsoft Authenticator-app.

Windows Hello
Het is waar mogelijk verplicht voor de gebruiker om Windows Hello te activeren, bijvoorbeeld d.m.v. een pincode of biometrie. Alle overige devices worden via Microsoft Intune gemonitord of zij hieraan voldoen.

Patchmanagement
Alle endpoints (workstations, laptops en servers) worden periodiek voorzien van de nieuwste updates. Dit gebeurt voor (kritieke) servers op vaste nachtelijke tijden en eventueel in overleg met de stakeholders. In geval van spoed worden de stakeholders hierover geïnformeerd.

Encryptie
Alle in- en externe gegevensdragers van endpoints (workstations, laptops en servers) zijn geëncrypt. Cryptografische worden geautomatiseerd beheerd.

Data Warehousing
Het gehele Data Warehouse van DHD is ondergebracht in Microsoft Azure (IT Onderaannemer) op basis van verschillende Azure Services.

Back-up protocol
Per component is een back-up protocol beschreven. Hierin zijn de retentie, storage type, back-up locatie en herstelpunten beschreven. Hierdoor wordt elk component op een passende wijze geback-upt.

Kritieke componenten worden in de vorm van snapshots geback-upt en op meerdere locaties bewaard met een retentie van 7 tot 90 dagen. Afwijkingen in de back-up worden dagelijks gemonitord.

Segmentatie
Het netwerk van DHD is gesegmenteerd. Dit betekent dat er een scheiding gemaakt tussen de omgevingen van de gebruikers, de kantoorautomatisering en de BI-omgeving. Deze omgevingen zijn in lijn met de classificatie van data.

DHD Zorg voor data

Zorg voor data

Webapplicaties

Webapplicaties

Power BI
Voor de webapplicaties vormt Power BI de basis voor het weergeven van de statistieken en analyses die de klanten kunnen samenstellen.

Encryptie
Alle gegevens worden versleuteld getransporteerd via up-to-date encryptiestandaarden. Gegevens worden niet fysiek getransporteerd. Alle certificaten worden beheerd door de afdeling IT&O.

Accounts en wachtwoorden
De accounts en wachtwoorden worden beheerd door de klant zelf. Hiervoor wijzen zij een lokaal beheerder aan. Het resetten en herstellen van accounts en wachtwoorden gebeurt bij voorkeur door de lokaal beheerder. Nieuwe accounts worden afgegeven met een eenmalig wachtwoord, waarna de gebruiker zelf een wachtwoord kan kiezen. DHD voert elke 6 maanden een controle op de accounts uit. De federatie van accounts is op dit moment nog niet mogelijk, hiermee wordt wel getest en zal op termijn beschikbaar komen.

Logging en auditing
Alle log- en auditingbestanden worden zorgvuldig opgeslagen. De bestanden zijn beveiligd tegen ongeautoriseerde toegang. De logging en auditing is zodanig gedetailleerd dat deze herleidbaar is naar natuurlijke personen.

Patchmanagement en CVE’s
Er wordt proactief gemonitord op nieuwe updates en CVE’s. Deze worden geïnstalleerd op vaste nachtelijke tijden of in overleg met de klanten. End-of-life applicaties worden niet gebruikt. De webapplicaties worden continue via Microsoft Defender for Cloud gemonitord en met regelmaat onderworpen aan een Vulnerability Scan. Aangetroffen kwetsbaarheden worden met de hoogste prioriteit opgelost.

Ontwikkelproces
Bij de ontwikkeling van webapplicaties wordt de OTAP-methodiek toegepast. Hierdoor zijn alle fases technisch van elkaar gescheiden. Hierbij zijn de principes van Security & Privacy by Design leidend.

Voordat een geheel nieuwe webapplicatie definitief in productie gaat, wordt deze eerst onderworpen aan een pentest door een externe partij.

Tijdschema onderhoud
Onderhoud aan de infrastructuur vindt elke maandagavond plaats. Updates van informatieproducten gaan per release. Hierover wordt er bij grote releases vroegtijdig gecommuniceerd met de stakeholders.

DHD Zorg voor data

Zorg voor data

Leveranciers & aanvullende informatie

Vereisten leveranciers

Certificering
De leverancier is in het bezit van tenminste een geldig ISO27001 en/of NEN7510-certificaat óf voldoet daaraan én is in staat deze op korte termijn te behalen.

Screening
DHD verwacht dat leverancier medewerkers steekproefsgewijs screent tijdens het sollicitatieproces d.m.v. een VOG, referentiecheck en social media-check.

Wachtwoordbeleid
DHD verwacht dat de medewerkers kunnen inloggen bij de leverancier aan de hand van een wachtwoordbeleid dat tenminste overeenkomt met dat van DHD.

Encryptie
DHD verwacht dat data(verkeer) wordt geëncrypt en voldoet aan de standaarden zoals AES en SHA-256. Het uitwisselen van gegevens gebeurt uitsluitend via een versleutelde en veilige HTTPS- en TLS-verbinding.

Beleid en (technische) maatregelen
Het beleid en (technische) maatregelen dat de leverancier hanteert, komt overeen met hoe DHD dat voor haarzelf heeft beschreven in dit document.

Aanvullende informatie

Privacy Statement
DHD heeft haar Privacy Statement online gepubliceerd. Deze kunt u hier lezen.

Nieuwsbrief
Wanneer u zich wilt aanmelden voor onze nieuwsbrief, kan dat via deze link. De DHD-nieuwsbrief verschijnt ongeveer 7 keer per jaar.

Verklaring van Toepasselijkheid
Wanneer u een kopie van het certificaat of de Verklaring van Toepasselijkheid wilt ontvangen, kunt u deze schriftelijk opvragen via ib@dhd.nl.

Disclaimer
Alle rechten zijn voorbehouden. DHD kan niet aansprakelijk worden gehouden voor fouten of onjuistheden in dit document.

Vragen
Heeft u vragen? Neem dan contact met ons op via de contactgegevens in dit document.

DHD Zorg voor data

030 799 61 65

info@dhd.nl

www.dhd.nl

Zorg voor data