

Veiligheid

De maatregelen die Archive-IT neemt voor optimale informatiebeveiliging, fysiek en digitaal.

Inhoud

Fysieke beveiliging	2
Digitale beveiliging	4
ISO certificaten	7
AVG, bewustwording & FG	8
Referenties	10
Over Archive-IT	11
Contact	12

Fysieke beveiliging

Archive-IT zet zich voortdurend in voor de optimale beveiliging van de fysieke archieflocaties. We nemen diverse maatregelen voor de bescherming van fysieke documenten en dossiers, zoals strikte toegangscontrole met badges, camerabewaking en doeltreffende inbraakpreventiesystemen om de documenten en dossiers te beschermen. Bovendien is er een directe doormelding naar de brandweer wanneer het brandalarm afgaat.

Vervoer

Veiligheid begint bij de bron. Tijdens het ophalen van dossiers plaatst Archive-IT deze in daarvoor bestemde trolleys en worden ze in verzegelde vrachtwagens naar één van onze beveiligde locaties vervoerd.

Beveiligde panden

Onze archieflocaties zijn speciaal ontworpen voor het opslaan van privacygevoelige archieven, met procedures die zorgvuldigheid, veiligheid en efficiëntie waarborgen. Dit betekent dat onze faciliteiten zijn ingericht met specifieke maatregelen voor optimale opslagcondities.



Fysieke beveiliging

Brandbeveiliging

De archiefruimtes zijn alleen bereikbaar via een sluis en uitsluitend toegankelijk voor geautoriseerde medewerkers. Fysieke documenten worden opgeslagen in compartimenten met brandvertragende deuren voor maximale bescherming. Daarnaast zorgen geavanceerde branddetectiesystemen en een CO2-blusgassysteem voor extra veiligheid, waardoor de beschikbaarheid van de dossiers te allen tijde gegarandeerd blijft.

Inbraakbeveiliging

Naast brandveiligheid, beschikken de panden over uitgebreide inbraakpreventiesystemen. Strikte toegangscontrole zorgt ervoor dat alleen bevoegd personeel toegang heeft tot relevante ruimtes. Bovendien zijn alle locaties voorzien van camerabewaking, zodat potentiële dreigingen snel worden opgemerkt.

Toegangscontrole

We hanteren een strikte toegangscontrole bij binnenkomst. Het is voor bezoekers niet mogelijk om zelfstandig binnen te komen of de archieflocaties te betreden. Bij binnenkomst dienen ze zich te melden en ontvangen ze na registratie een badge. Deze badge dient men zichtbaar te dragen.





Digitale beveiliging

Naast fysieke beveiliging is digitale veiligheid van uiterst belang. Dit staat voorop in onze softwareoplossingen. Ook maken wij gebruik van externe partijen om onze digitale veiligheid te waarborgen.

Softwareoplossingen

Onze software biedt diverse mogelijkheden en maatregelen om de veiligheid optimaal te waarborgen.

Toegangsbeveiliging

In onze softwareoplossingen passen we verschillende veiligheidsmaatregelen toe om data te beschermen. We maken gebruik van sterke wachtwoorden en Two Factor Authentication (2FA), waarbij gebruikers een extra verificatiestap moeten doorlopen om toegang te krijgen. Dit maakt het voor onbevoegden veel moeilijker om toegang te krijgen.

Need-to-know

Onze software werkt met groepen-rollen-rechten waarbij rechten tot in detail kunnen worden vastgelegd. Toegang en rechten worden bepaald op basis van het need-to-know principe. Via logging kunnen alle activiteiten binnen onze software worden gevolgd. Het openen, wijzigen of verwijderen van documenten wordt zorgvuldig geregistreerd, waarna deze geanalyseerd kunnen worden op onregelmatigheden.

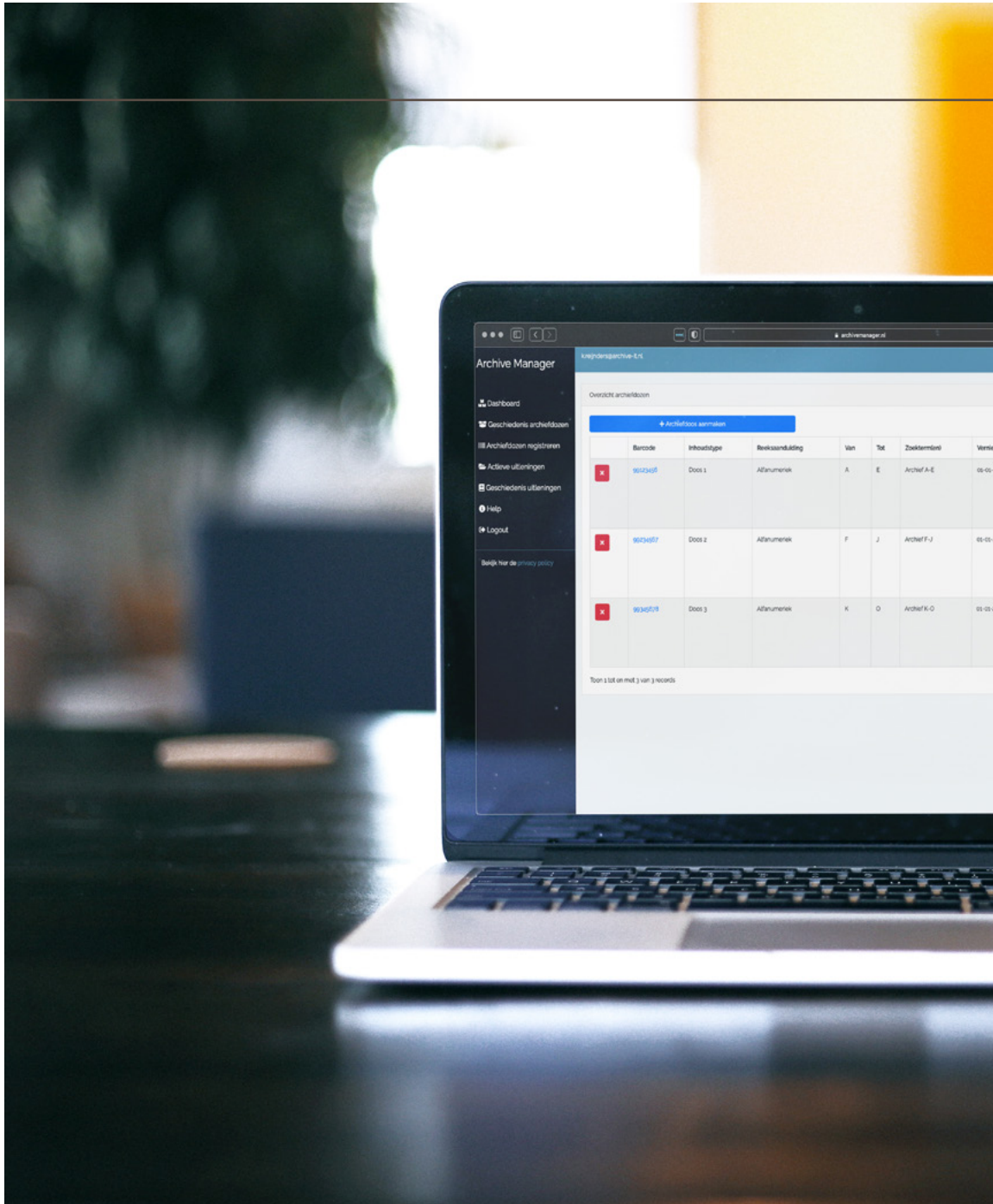
Digitale beveiliging

Intermax

De gedigitaliseerde gegevens en onze softwareoplossingen zijn ondergebracht bij Intermax Cloudsourcing. Intermax levert hoogwaardige technologieoplossingen aan klanten. Daarnaast voldoet Intermax aan de strengste normen en is het bedrijf in bezit van certificaten die op onze branche van toepassing zijn. Zo zorgt Intermax voor een zo goed mogelijke beveiliging van gegevens tegen ongeoorloofde toegang, wijziging, diefstal of beschadiging.

Serverbeveiliging

De beveiliging van onze servers wordt dagelijks proactief gecontroleerd met de Guardian360 security scan. Onze softwareoplossingen worden ontwikkeld volgens het 'security by design' principe. Hierbij volgen we richtlijnen die meestal overeenkomen met de richtlijnen van het NCSC. Daarnaast wordt de software periodiek gecontroleerd door een externe gecertificeerde partij op kwetsbaarheden, door middel van penetratietests.





Digitale beveiliging

Ethische hacking

Archive-IT maakt regelmatig gebruik van externe pentesten door daartoe gespecialiseerde partijen. Onze applicaties worden actief getest door gecontroleerde aanvallen uit te voeren om zwakke plekken te identificeren. Deze aanpak stelt ons in staat om beveiligingslekken op te sporen en te verhelpen, zodat misbruik wordt voorkomen. Dit voortdurende proces zorgt ervoor dat onze systemen altijd worden verbeterd en aangepast aan de nieuwste dreigingen, zodat we de maximale beveiliging van uw waardevolle gegevens kunnen waarborgen.

ISO Certificaten

Archive-IT heeft haar processen rondom de beveiliging van zowel fysieke als digitale dossiers optimaal op orde, wat onder andere blijkt uit de certificeringen die zijn afgegeven na onafhankelijke audits. De ISO-certificaten zijn een onmisbaar aspect geworden voor Archive-IT.

Archive-IT is gecertificeerd voor verschillende ISO- en NEN-certificaten:

ISO 27001

Informatiebeveiliging



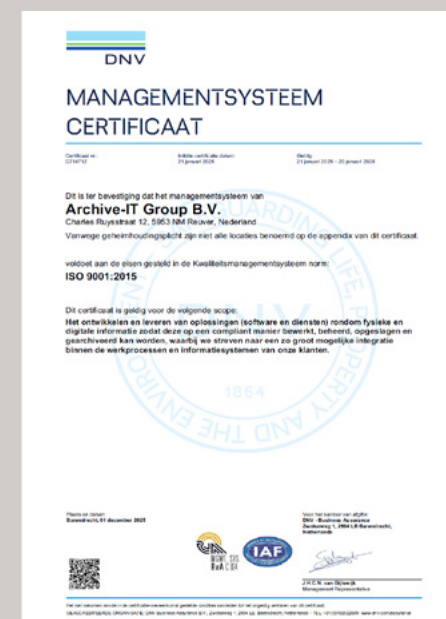
NEN 7510

Informatiebeveiliging in de zorgsector



ISO 9001

Kwaliteitsmanagement van de processen





AVG, FG, & bewustwording

Naast de ISO- en NEN-certificeringen, is de Algemene Verordening Gegevensbescherming (AVG) van groot belang. Andere belangrijke aspecten zijn de Functionaris Gegevensbescherming en bewustwording van onze medewerkers.

AVG

Archive-IT verwerkt dagelijks vele dossiers, boordevol privacygevoelige informatie. Toen de AVG werd geïntroduceerd, heeft Archive-IT zich daar volledig op gericht, en met trots kunnen wij zeggen dat wij AVG-compliant zijn. Dit is van groot belang voor onze klanten, die hun waardevolle en privacygevoelige informatie aan ons toevertrouwen.

Functionaris Gegevensbescherming

Een belangrijk onderdeel van de AVG is de verplichting tot het aanstellen van een Functionaris Gegevensbescherming (FG). De externe FG voor Archive-IT is drs A.E. Klaassen. Hij is Managing Partner bij NewDay IT Risk & Assurance Services. Alex Klaassen is ingeschreven bij de Autoriteit Persoonsgegevens en heeft namens hen een toezichthoudende rol binnen Archive-IT.

Contact

De heer Drs A. (Alex) E. Klaassen RE CIPP/E CIPM
Registratienummer: FG003942
E-mail: alex.klaassen@newdayriskservices.nl



AVG, FG, & bewustwording

Bewustwording

Bewustwording rondom dit thema staat bij Archive-IT hoog op de agenda. Zo is een van de onderdelen bij het introductieprogramma voor nieuwe medewerkers een sessie over kwaliteit, informatiebeveiliging en privacy. Daarnaast vindt er periodiek bewustwording onder de huidige medewerkers plaats in de vorm van e-mailberichten die inspelen op de actualiteit, privacy als thema in de kwartaaloverleggen en periodieke toetsen. De veranderende wet- en regelgeving wordt nauwlettend in de gaten gehouden en waar nodig worden procedures en/of maatregelen aangepast.

Referenties



zuyderland

**Wiggers
Faber** | advocaten-
belastingkundigen



gemeente Langedijk

Jacques van Kerkvoort Programmamanager

“Tijdens het bedrijfsbezoek aan Archive-IT waren we zo onder de indruk van de manier waarop Archive-IT ervoor zorgt dat dossiers, zowel fysiek als digitaal, beveiligd worden, dat voor ons de keuze snel gemaakt was.”

Debora Janssen Juridisch secretaresse

“Als je ziet wat Archive-IT aan maatregelen neemt om de informatiebeveiliging op hoog niveau te krijgen en te houden, dan weet je: voor service, kwaliteit en zorgvuldigheid moet je bij Archive-IT zijn.”

Alex Huisman Adviseur Informatisering & Automatisering

“De keuze voor Archive-IT werd genomen na een gedegen onderzoek. Een belangrijk criterium was het ISO 27001 certificaat. Er wordt met privacygevoelige documenten gewerkt en Archive-IT heeft dat helemaal op orde.”



Over Archive-IT

Archive-IT is de betrouwbare partner voor organisaties die grip willen krijgen op hun informatiebeheer en klaar willen zijn voor de toekomst. Ons hoofdkantoor is gevestigd in het Limburgse Reuver. Daarnaast hebben wij vestigingen in Raamsdonksveer en Hoogezand (NL), België, Duitsland en Frankrijk. Wij zijn ontstaan vanuit Jalema, producent op het gebied van archief- en kantoorartikelen, en kennen de archiveringswereld daarom als geen ander.

Wij bieden slimme, veilige en innovatieve oplossingen die fysieke en digitale archivering naadloos combineren en eenvoudig integreren met moderne digitale werkomgevingen. Met onze integrale aanpak - van procesoptimalisatie tot volledig compliant informatiemanagement - maken wij het verleden toegankelijk, voldoen we aan de eisen van het heden en bereiden we u voor op een digitale, duurzame toekomst.

Contact

Wilt u meer inzicht in onze veiligheidsmaatregelen of ontdekken hoe wij deze specifiek kunnen toepassen binnen uw organisatie? Onze experts bij Archive-IT staan klaar om met u mee te denken over een maatwerkoplossing.

Wij helpen u niet alleen bij het waarborgen van veiligheid, maar ook bij het gestructureerd en overzichtelijk beheren van uw informatie. Of het nu gaat om digitale archivering, compliance of risicobeheersing, wij bieden u de juiste ondersteuning.

Archive-IT
Charles Ruysstraat 12
5953 NM Reuver

+31 77 750 11 00
info@archive-it.nl
www.archive-it.nl



Vraag een adviesgesprek aan met één van onze ervaren adviseurs. Stuur een mail naar info@archive-it.nl, bel naar 077 750 11 00 of plan een gesprek in via onderstaande button. Wij helpen u graag verder!

Adviesgesprek inplannen

Archive-IT streeft er naar om zo goed mogelijk op de hoogte te blijven van de wet- en regelgeving. Desondanks kan aan de inhoud van dit document geen rechten worden ontleend.