Kiteworks

COMPLIANCEBRIEF

VOOR NEDERLANDSE ZORGORGANISATIES

Zivver en Kiteworks zijn gecertificeerd voor NEN 7510-1:2024 — Medische informatica — Informatiebeveiliging in de zorg — Deel 1: Managementsysteem

Van zero-trust-architectuur tot realtime SIEM-feeds: een technisch pad door de verplichtingen van de Nederlandse zorg rond persoonlijke gezondheidsinformatie

NEN 7510-1:2024 | Nederlandse Zorg | Zivver + Kiteworks

Oplossingshighlights

- Sterke Dubbele Encryptie
- Data Policy Engine met ABAC en RBAC
- SafeEDIT
- SafeVIEW
- Uitgebreide audit logs met SIEM-feeds
- eDiscovery-toegangscontroles

NEN 7510-1:2024, getiteld "Medische informatica — Informatiebeveiliging in de zorg — Deel 1: Managementsysteem," is een Nederlandse nationale norm die in 2024 door NEN is gepubliceerd en die een informatiebeveiligingsmanagementsysteem voor de zorg vaststelt. De norm is van toepassing op zorgaanbieders, zorginstellingen en verwerkers van persoonlijke gezondheidsinformatie — ziekenhuizen, instellingen voor langdurige zorg, organisaties voor geestelijke gezondheidszorg, solistisch werkende zorgverleners en leveranciers van zorginformatiesystemen — ongeacht omvang, overal in Nederland.

De norm legt geen geldboetes op; naleving vloeit voort uit vereisten in de hoofdstukken 4 tot en met 10 en bijlage A, met handhaving via de Nederlandse zorgregelgeving, verzekerings- en overheidscontracten, en toezicht door de Autoriteit Persoonsgegevens, met als risico sancties, verlies van certificering en contractuele aansprakelijkheid. Zivver, nu onderdeel van Kiteworks, wordt genoemd in Certificaat NL 3069.1.1: Brand Compliance B.V., een Nederlandse door de RvA geaccrediteerde instantie (RvA C 548), heeft geverifieerd dat het ISMS van Zivver Secure Communications Services voldoet aan NEN 7510-1:2024, geldig van 6 augustus 2026 tot en met 31 juli 2029. Kiteworks bezit deze certificering en ondersteunt organisaties die hun eigen compliance nastreven.

NEN 7510-1:2024 Zero-Trust-Architectuur Sluit Aan Bij Nederlandse Zorgbescherming

NEN 7510-1:2024 vereist toegangsbeheer, versleutelde gezondheidsinformatie, fysieke beveiligingsmaatregelen en veilige ontwikkelpraktijken. De ABAC/RBAC-controles van de Data Policy Engine en standaardinstellingen voor minimale toegangsrechten regelen de gegevenstoegang; SCIM, LDAP/SAML SSO en extern-gebruikersbeheer automatiseren de identiteitscyclus. Meervoudige authenticatie, verplicht voor systemen die persoonlijke gezondheidsinformatie verwerken (A.8.5), verloopt via RADIUS, PIV/CAC en OTP, naast RBAC-maprollen en vervalinstellingen. Encryptie in rust versleutelt elk bestand dubbel; Customer-owned keys en HSM-integratie houden de sleutelbeheer bij de organisatie; en FIPS 140-3 gevalideerde encryptie voldoet aan de verplichting om verwijderbare media en back-ups te versleutelen (A.7.10, A.8.13). SafeVIEW toont gedeelde bestanden als watermerkafbeeldingen die alleen kunnen worden bekeken, zodat persoonlijke gezondheidsinformatie kan worden ingezien zonder te worden gekopieerd, gedownload of doorgestuurd, terwijl SafeEDIT geautoriseerde gebruikers in staat stelt diezelfde bestanden te bewerken binnen een virtuele desktop die naar de browser wordt gestreamd, zodat het bestand zelf de beveiligde Kiteworks-omgeving nooit verlaat; encryptie in transit beveiligt beide sessies, en admin- en eindgebruikersrollen handhaven functiescheiding. Tiered internal services, zero trust mode, embedded firewalls, AI-based intrusion and anomaly detection en Fail2Ban vormen een zero-trust-perimeter, met antivirus, threat prevention, bestandssanering, hoge beschikbaarheid en uitgebreide Dev SecOps. Reikwijdte, beleid, risicoacceptatie, leveranciersovereenkomsten en personeelsverplichtingen van het ISMS blijven de verantwoordelijkheid van de organisatie.

Doelstellingen Ondersteund Door DPE en Compliancerapporten

NEN 7510-1:2024 vereist een voortdurend verbeterend informatiebeveiligingsmanagementsysteem, meetbare doelstellingen, periodieke risicobeoordelingen en doorlopende controle-monitoring, plus toezicht op wijzigingen bij leveranciers. De ABAC- en RBAC-controles van de Data Policy Engine geven invulling aan de toegangsbeheerdimensie van de norm, terwijl compliancerapporten over audit logs, interne en externe dreigingen, GDPR en HIPAA meetbaar bewijs leveren van de effectiviteit van de controles. Uitgebreide audit logs met SIEM-feeds, genormaliseerd tot één stroom, leveren het bewijsmateriaal dat risicobeoordelaars nodig hebben. Op rollen gebaseerde admintoegang tot trackinggegevens wijst een specifieke compliancerol toe, waardoor taken worden gescheiden, en de exporteerbare activiteits- en gebruiksrapporten van admin reporting laten zien wat er gemonitord moet worden en hoe dit te valideren is. Leveranciersbeveiligingsmonitoring maakt gebruik van dezelfde geconsolideerde logs en compliancerapporten. Datasoevereiniteit en geofencing voldoen aan de cloudgovernance-vereiste van de norm (A.5.23) door gegevens uitsluitend op te slaan en te routeren binnen het toegewezen land van een gebruiker, met residency-rapportage; Customer-owned keys en Single-tenant private cloud behouden de sleutelbeheer en databaseïsolatie, ongeacht het implementatiemodel.

Incidentdetectie, Bewijsbehoud en Kwetsbaarheidsopvolging

NEN 7510-1:2024 vereist dat organisaties beveiligingsgebeurtenissen beoordelen, incidenten afhandelen via gedocumenteerde procedures, bewijs bewaren, medewerkers een manier bieden om vermoedelijke gebeurtenissen te melden, netwerken monitoren op afwijkingen, logbestanden analyseren (A.8.15), klokken synchroniseren, kwetsbaarheden en capaciteit bijhouden, en threat intelligence onderhouden. Uitgebreide audit logs met SIEM-feeds voegen elke beveiligingsgebeurtenis samen tot één ongedempte stroom, die in realtime wordt gevoed aan ArcSight, QRadar, Splunk en LogRhythm. AI-based intrusion and anomaly detection en gelogde topics identificeren verdachte activiteit, terwijl security analytics via het CISO Dashboard afwijkingen zichtbaar maakt voordat ze tot een inbreuk leiden. Wanneer een gebeurtenis escaleert tot een incident, ondersteunen log export feeds, het compliancerapport voor interne dreigingen, en embedded managed detection and response de gedocumenteerde respons. Trusted audit logs en Legal hold- en eDiscovery-toegangscontroles, beperkt tot Data Leak Investigator Admins, bewaren bewijs (A.5.28). Secure Data Forms bieden medewerkers een meldkanaal; NTP-kloksynchronisatiecontroles en SNMP Health Monitoring met de Node Health API houden tijdstempels, capaciteit en kwetsbaarheden bij.

Kiteworks voldoet aan de verplichtingen van NEN 7510-1:2024 voor de bescherming van persoonlijke gezondheidsinformatie door middel van dubbele encryptie in rust en in transit, possessionless editing via SafeEDIT, datamaskering via SafeVIEW, DLP-integratie en een zero-trust-netwerkarchitectuur die wederzijdse authenticatie afdwingt op elke servicegrens. De ABAC- en RBAC-controles van de Data Policy Engine, SCIM-gestuurd identiteitsbeheer en verplichte meervoudige authenticatie geven invulling aan de rolgebaseerde toegangs- en identiteitsregistratie-eisen van de norm voor systemen die persoonlijke gezondheidsinformatie verwerken. Uitgebreide audit logs met SIEM-feeds, AI-based Intrusion and Anomaly Detection, legal hold-controles en compliancerapporten voor interne/externe dreigingen bieden zorgorganisaties de continue monitoring, incidentrespons en bewijsbehoudmogelijkheden die de norm vereist. Kiteworks functioneert als een uniform platform voor bescherming, toegangsbeheer en beveiligingsoperaties voor organisaties die conformiteit met NEN 7510-1:2024 nastreven.

Ontdek Hoe Kiteworks Uw NEN 7510-1:2024 Compliancetraject Ondersteunt

www.kiteworks.com

Kiteworks

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.