



RELINED
FIBER NETWORK

Informatiebeveiliging,
digitale weerbaarheid en
ketenveiligheid.

Relined Fiber Network

Praktische beveiligingsmaatregelen van toepassing op Partijen voor zover relevant voor de uitvoering van de overeenkomst. Deze maatregelen zijn uitsluitend van toepassing voor zover relevant en passend gelet op de aard van de werkzaamheden, de verleende toegang en de daarmee samenhangende risico's. De meest actuele versie van deze bijlage is beschikbaar via: <https://relined.eu/beleid-documenten/>

1. Doel en toepasselijkheid

Dit document ondersteunt de bescherming van informatie, systemen, infrastructuur en dienstverlening van Relined en draagt bij aan de digitale weerbaarheid en beveiliging van de toeleveringsketen. De maatregelen zijn gericht op de vertrouwelijkheid, integriteit, beschikbaarheid en authenticiteit van informatie en diensten en zijn mede opgesteld ter ondersteuning van de verplichtingen die voor Relined gelden op grond van de Cyberbeveiligingswet en daarop gebaseerde regelgeving.

2. Algemene beveiligingsmaatregelen

- Passende technische, organisatorische en risicogebaseerde maatregelen toepassen.
- Passende werkafspraken of procedures voor informatiebeveiliging hanteren.
- Relevante beveiligingsrisico's periodiek beoordelen.
- Waar nodig corrigerende maatregelen treffen.
- Verantwoordelijkheden voor informatiebeveiliging passend beleggen binnen de organisatie.

3. Bescherming van informatie, systemen en toegang

- Informatie uitsluitend gebruiken voor de uitvoering van de overeenkomst.
- Toegang beperken tot personen die deze informatie daadwerkelijk nodig hebben.
- Beveiligingsgevoelige informatie beschermen tegen verlies, diefstal, onbevoegde toegang, wijziging of openbaarmaking.
- Accounts persoonlijk gebruiken en (inloggegevens) niet delen (met onbevoegden).
- Wachtwoorden en andere authenticatiemiddelen vertrouwelijk behandelen.
- Multifactorauthenticatie gebruiken – waar relevant –, waarbij naast een wachtwoord een aanvullende verificatiemethode wordt gebruikt, zoals een authenticator-app, beveiligingscode of hardwaretoken.
- Toegang direct beëindigen zodra deze niet meer nodig is.
- Bijzonder zorgvuldig omgaan met glasvezeltracés, GIS-gegevens, netwerkinformatie, tekeningen, technische documentatie, HUB- en POP-gegevens, toegangsgegevens en projectinformatie.

4. Personeel, bewustwording en cyberhygiëne

- Medewerkers instrueren over relevante beveiligingsrisico's.
- Phishing, social engineering, verdachte links, malware en frauduleuze verzoeken herkennen en melden.
- Actuele antivirus- of endpointbescherming gebruiken waar relevant.
- Beveiligingsupdates tijdig installeren.
- Sterke wachtwoorden gebruiken.
- Apparatuur vergrendelen en zorgvuldig omgaan met mobiele apparaten en gegevensdragers.

5. Technische beveiliging

- Patchmanagement en kwetsbaarhedenbeheer uitvoeren waar relevant.
- Bescherming tegen malware toepassen.
- Logging en monitoring toepassen waar relevant voor gebruikte of beheerde systemen.
- Versleuteling toepassen waar passend.
- Back-up- en herstelmaatregelen toepassen indien hiervoor verantwoordelijk.

- Bij levering of beheer van software, hardware of digitale diensten passende beveiligingsupdates en onderhoud uitvoeren.

6. Fysieke toegang en locaties

- Voor zover een Partij toegang krijgt tot POP's, datacenters, technische ruimtes of andere beveiligde locaties van de andere Partij uitsluitend gebruiken voor de overeengekomen werkzaamheden.
- Alleen bevoegde personen toegang geven.
- Toegangsmiddelen niet delen met onbevoegden.
- Toegangs- en veiligheidsinstructies van Relined danwel de eigenaar van de locatie naleven.
- Verlies of vermoed misbruik van toegangsmiddelen direct melden.

7. Beveiligingsincidenten

- Beveiligingsincidenten of vermoedens daarvan zonder onnodige vertraging melden aan de Security Officer van Relined; so@relined.eu
- Voor zover redelijkerwijs mogelijk een eerste melding doen binnen 24 uur nadat het incident bekend is geworden.
- Ook incidenten bij betrokken onderaannemers, leveranciers of dienstverleners melden indien deze gevolgen kunnen hebben voor Relined.
- Melden wat bekend is over aard, impact en getroffen maatregelen.
- Relevante updates verstrekken zodra aanvullende informatie beschikbaar komt.

8. Ketenveiligheid

- Passende geheimhoudings- en beveiligingsafspraken opleggen aan onderaannemers, leveranciers of dienstverleners die betrokken zijn bij de werkzaamheden.
- Toegang van onderaannemers, leveranciers of dienstverleners tot informatie en locaties beperken tot wat noodzakelijk is.
- Relevante beveiligingsmaatregelen uit deze bijlage doorleggen aan betrokken derden.

9. Continuïteit en herstel

- Passende maatregelen treffen voor continuïteit van werkzaamheden.
- Herstel na (cyber)verstoringen ondersteunen.
- Voorbereid zijn op cyberincidenten en andere ernstige verstoringen voor zover relevant voor de continuïteit van werkzaamheden.
- De andere Partij zo spoedig mogelijk informeren bij ernstige verstoringen die de veiligheid, beschikbaarheid van informatie danwel de werkzaamheden kunnen beïnvloeden.

10. Verificatie en bewijs

- Op redelijk verzoek informatie verstrekken waaruit blijkt welke relevante beveiligingsmaatregelen worden toegepast
- Indien beschikbaar kan dit bestaan uit certificeringen, procedures, audit- of assurance informatie, informatie over patchmanagement en/of antwoorden op beveiligingsvragenlijsten.
- Meewerken aan redelijke verificatie wanneer sprake is van een concreet beveiligingsrisico.

11. Contactpersonen

- Actuele operationele en beveiligingscontacten beschikbaar houden.
- Beschikken over een contactpunt voor beveiligingsincidenten en urgente beveiligingskwesties.