



RELINED
FIBER NETWORK

Information security, cyber
resilience and supply chain
security

Relined Fiber Network

Practical security measures applicable to Parties to the extent relevant to the performance of the Agreement. These measures apply solely to the extent relevant and appropriate, taking into account the nature of the activities, the access granted and the associated risks. The most recent version of this annex is available at: <https://relined.eu/beleid-documenten/>

1. Purpose and applicability

This document supports the protection of Relined's information, systems, infrastructure and services and contributes to cyber resilience and supply chain security. The measures are intended to safeguard confidentiality, integrity, availability and authenticity of information and services contribute to compliance with the obligations applicable to Relined pursuant to the Cybersecurity Act and any regulations promulgated thereunder.

2. General security measures

- Implement appropriate technical, organizational and risk-based security measures.
- Maintain appropriate information security practices and procedures.
- Periodically assess relevant security risks.
- Implement corrective measures where necessary.
- Assign responsibilities for information security appropriately within the organization.

3. Protection of information, systems and access

- Use information solely for the performance of the Agreement.
- Restrict access to individuals who have a legitimate need to know such information.
- Protect security-sensitive information against loss, theft, unauthorized access, alteration or disclosure.

- Use accounts on an individual basis and do not share accounts or login credentials with (unauthorized) persons.
- Treat passwords and other authentication credentials as strictly confidential.
- Use multi-factor authentication, where relevant, requiring an additional verification method in addition to a password, such as an authenticator application, security code or hardware token.
- Terminate access immediately once it is no longer required.
- Exercise particular care when handling fibre optic route information, GIS data, network information, drawings, technical documentation, HUB and POP information, access credentials and project information.

4. Personnel, awareness and cyber hygiene

- Instruct employees regarding relevant security risks.
- Identify and report phishing attempts, social engineering, suspicious links, malware and fraudulent requests.
- Use up-to-date antivirus or endpoint protection where relevant.
- Install security updates in a timely manner.
- Use strong passwords.
- Secure devices when unattended and exercise due care in the use of mobile devices and data storage media.

5. Technical security

- Perform patch management and vulnerability management where relevant.
- Implement protection against malware.
- Apply logging and monitoring where relevant to the systems used or managed.
- Use encryption where appropriate.
- Implement backup and recovery measures where responsible for doing so.
- When supplying or managing software, hardware or digital services, implement appropriate security updates and maintenance.

6. Physical access and locations

- To the extent a Party is granted access to POPs, data centres, technical facilities or other secure locations of the other Party, such access shall be used solely for the agreed activities.
- Grant access only to authorized persons.
- Do not share access credentials or access devices with (unauthorized) persons.

- Comply with the access and security instructions issued by Relined and/or the owner of the relevant location.
- Immediately report any loss of, or suspected misuse of, access credentials or access devices.

7. Security incidents

- Report security incidents, or any suspected security incidents, to Relined's Security Officer without undue delay at: so@relined.eu
- To the extent reasonably possible, submit an initial notification within twenty-four (24) hours after becoming aware of the incident.
- Also report incidents involving subcontractors, suppliers or service providers where such incidents may impact Relined.
- Provide all known information regarding the nature of the incident, its impact and any mitigation measures taken.
- Provide relevant updates as soon as additional information becomes available.

8. Supply chain security

- Impose appropriate confidentiality and security obligations on subcontractors, suppliers and service providers involved in the activities.
- Restrict subcontractor, supplier and service provider access to information and locations to what is strictly necessary.
- Ensure that involved third parties adhere to relevant security measures set out in this document.

9. Business continuity and recovery

- Implement appropriate measures to ensure the continuity of activities.
- Support recovery following cyber incidents and other disruptions.
- Maintain preparedness for cyber incidents and other serious disruptions to the extent relevant to the continuity of activities.
- Inform the other Party as soon as reasonably practicable of any serious disruption that may affect security, the availability of information, or the performance of services.

10. Verification and evidence

- Upon reasonable request, provide information demonstrating which relevant security measures are being implemented.
- Where available, such information may include certifications, procedures, audit reports, assurance information, information concerning patch management and/or responses to security questionnaires.
- Cooperate with reasonable verification activities where a specific security risk has been identified.

11. Contact persons

- Maintain up-to-date operational and security contact details.
- Maintain a designated point of contact for security incidents and urgent security-related matters.