aginion

NIS2

Statement of Support and Readiness

Aginion Luxembourg

Date: 2026-06-12

Classification: Public

Purpose

This statement describes how Aginion Luxembourg ("we") aligns its security programme with the network- and information-security measures set out in the NIS2 Directive (Directive (EU) 2022/2555), as transposed in Luxembourg. It is provided for the information of our customers and prospective customers — particularly those who are themselves subject to NIS2 and must account for the security of their supply chain. It is not a contractual warranty.

Our status under NIS2

NIS2 was transposed in Luxembourg by the Law of 5 May 2026, which entered into force on 10 May 2026, designates the Institut Luxembourgeois de Régulation (ILR) as competent authority, and requires in-scope entities to self-register.

Based on our size, we fall below the thresholds at which an entity is in scope by default, and we have not been individually designated an essential or important entity. We are therefore not currently a regulated entity under NIS2 and have no registration obligation. Should our size or activity change so that we come within scope, or should we be individually designated, we will register with the ILR and meet the applicable obligations.

Voluntary alignment

Although not required to, we voluntarily align our security programme with the risk-management measures set out in Article 21 of NIS2. Our programme is certified to ISO/IEC 27001, whose controls cover the substance of these measures. In particular:

- Risk management and security policies — a documented information-security management system with regular risk assessment.
- Incident handling — detection, response, and recovery processes, described in our incident-response statement.
- Business continuity — backup, disaster recovery, and crisis management, maintained and tested regularly.
- Supply-chain security — assessment and management of security across our supplier and service-provider relationships.
- Secure acquisition, development, and maintenance — including vulnerability handling and a published vulnerability-disclosure policy.
- Effectiveness review — regular assessment of the effectiveness of our security measures, including independent penetration testing.
- Cyber hygiene and training — baseline security practices and staff security-awareness training.
- Cryptography — use of encryption for data in transit and at rest, in line with our policies.
- Access control, asset management, and personnel security — including least-privilege access and staff security measures.
- Strong authentication — multi-factor authentication for access to sensitive systems, and secured communications.

Incident reporting readiness

We are not subject to NIS2's reporting duties. Nonetheless, our incident-management process is designed to notify affected customers promptly and to operate on timelines consistent with the NIS2 reporting stages (early warning, incident notification, and final report), so that customers who are themselves in scope receive what they need to meet their own reporting obligations.

Supporting your NIS2 obligations

For customers subject to NIS2, we support your supply-chain security obligations by maintaining the measures above, cooperating with your security requirements and assessments, and providing information about our security posture on request.

Related documents

This statement should be read alongside our ISO/IEC 27001 certification, our incident-response statement, our business-continuity and disaster-recovery statement, and our vulnerability-disclosure policy.

Governance and review

This statement is reviewed at least annually, and sooner if triggered by a material change in our size, activity, security programme, or the applicable law.

- End of Document -

aginion

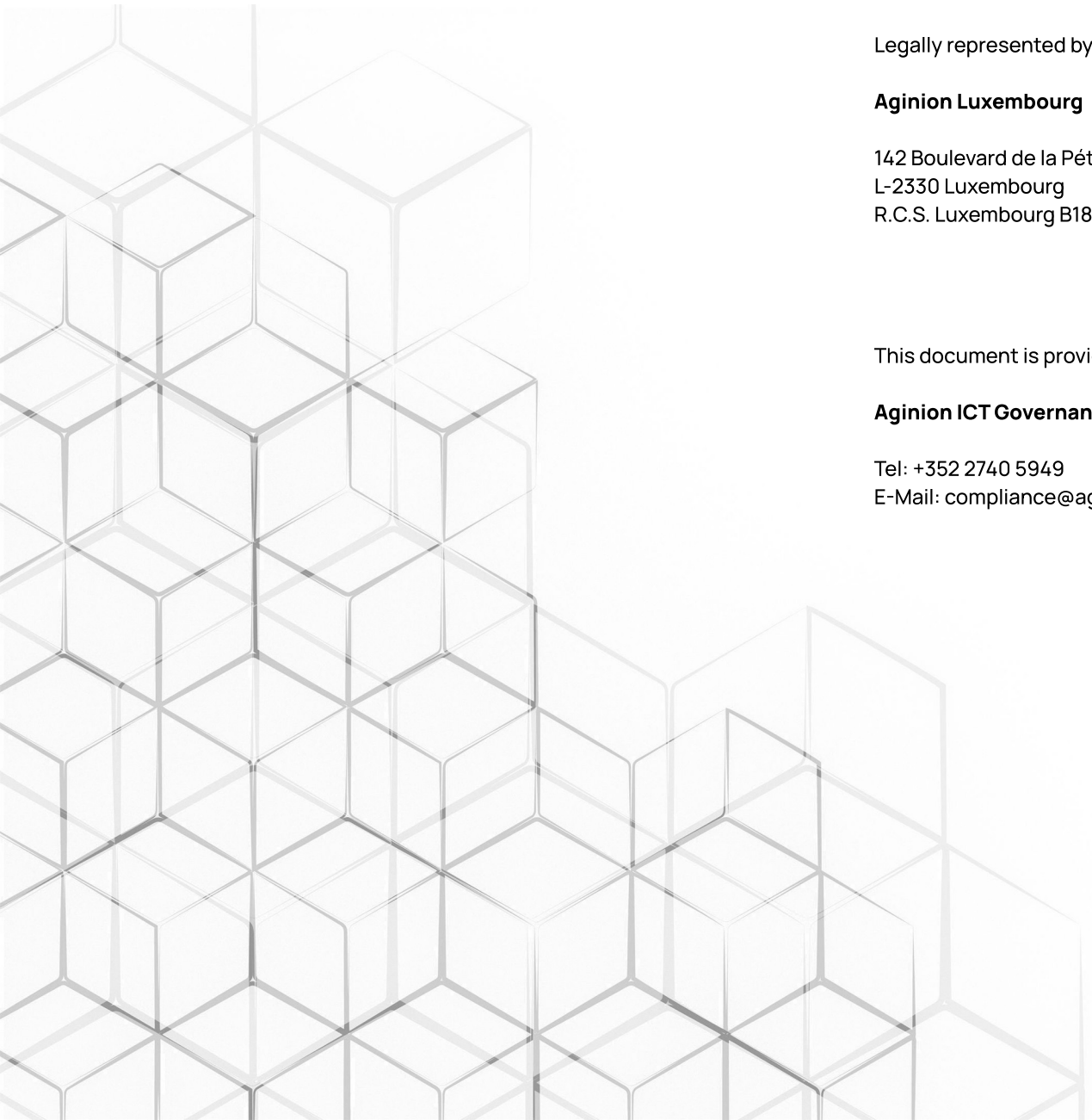
Aginion Group

Legally represented by:

Aginion Luxembourg

142 Boulevard de la Pétrusse
L-2330 Luxembourg
R.C.S. Luxembourg B184509

This document is provided by:

Aginion ICT Governance

Tel: +352 2740 5949
E-Mail: compliance@aginion.com