aginion

Business Continuity Statement

Aginion Luxembourg

Date: 2026-07-20

Classification: Public

Purpose

This statement describes how Aginion Luxembourg ("we") maintains the continuity of its services and recovers its systems and customer data in the event of disruption. It is provided for the information of our customers and prospective customers. It summarises our approach; it is not our internal business-continuity or disaster-recovery plan, and it is not a contractual warranty. Binding availability and recovery terms are set out in the applicable service agreement.

What our arrangements cover

We maintain documented business-continuity and disaster-recovery plans, owned by the Chief Information Security Officer (CISO), covering the continuity of our services and the recovery of systems and data following disruptions such as infrastructure or hardware failure, a cyber-security incident, loss of a facility, or failure of a key supplier.

Key elements

- Recovery objectives. We define recovery time objectives (RTO) and recovery point objectives (RPO) for our services, review them regularly, and test against them. The objectives applicable to a specific service are available to customers under the applicable agreement or on request.
- Backups. We take regular backups of systems and customer data and test our ability to restore from them as part of our recovery testing.
- Resilience. Our services are designed with resilience appropriate to their criticality, so that we can maintain or restore them within our recovery objectives.
- Crisis management. Defined roles and responsibilities govern how we manage a major disruption, coordinate our response, and communicate with affected customers.
- Continuous improvement. Findings from tests and from any real disruption are used to improve our plans and controls.

Testing

We test our business-continuity and disaster-recovery arrangements at least quarterly. Each test confirms whether our recovery objectives are met and whether any deviations require remediation. We publish a short summary report for each quarterly test, confirming that the test took place and its outcome, without disclosing details that could compromise the security of our environment.

Relationship to incident response

A disruptive security incident may trigger both our incident-response process and our disaster-recovery arrangements. This statement should be read alongside our incident-response statement.

Related documents

This statement should be read alongside our incident-response statement, our ISO/IEC 27001 certification, and — for the relevant customers — our DORA and NIS2 statements. The quarterly test-report summaries are published in our Trust Center on aginion.com.

Governance and review

This statement is reviewed at least annually, and sooner if triggered by a material change in our arrangements, our services, or the applicable law.

- End of Document -

aginion

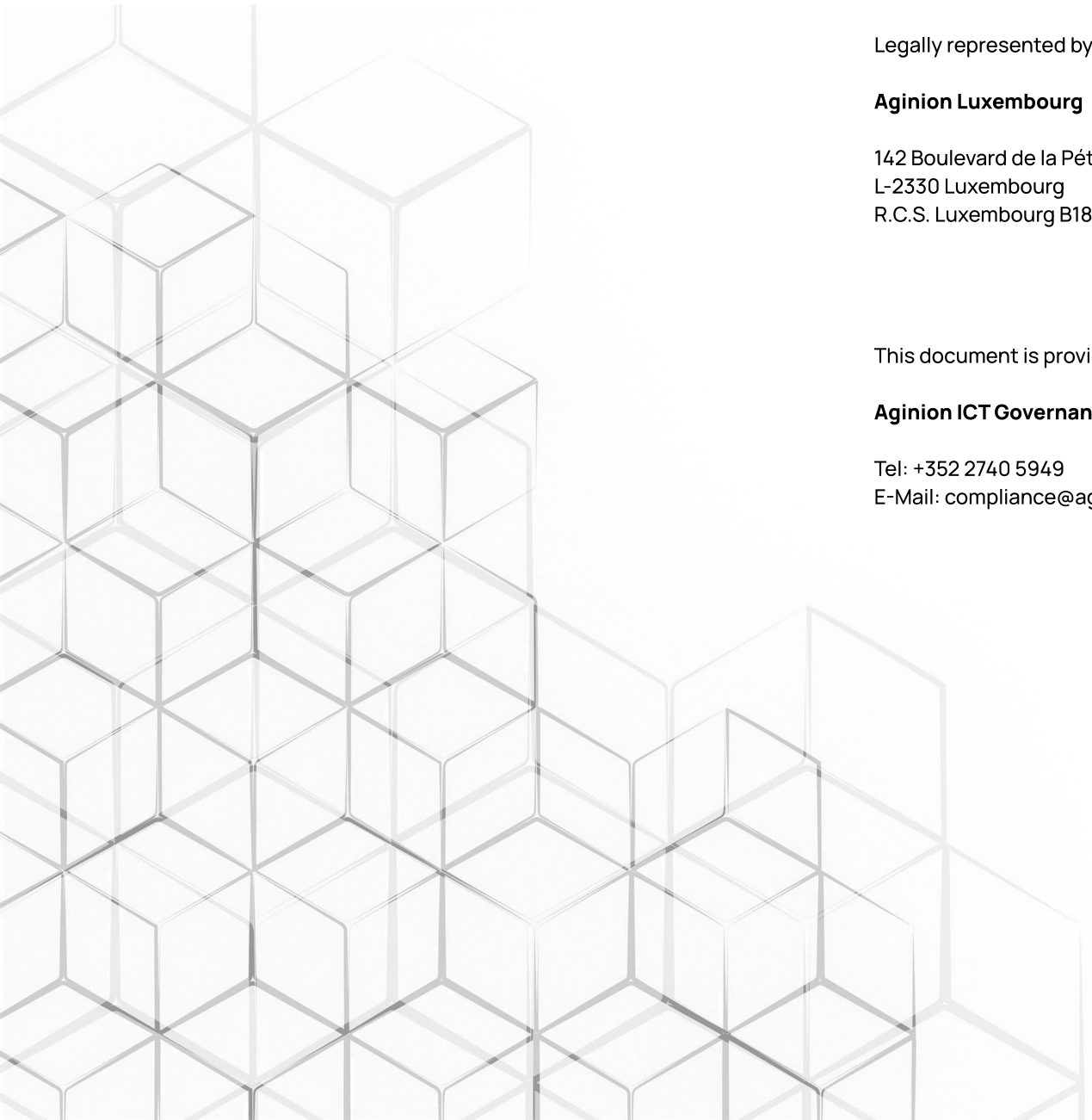
Aginion Group

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