DATA PROTECTION AND INFORMATION SECURITY POLICY

Mission and Scope

2Connect Telecommunications Infrastructure and Network Services Ltd. (hereinafter: the Company), as an independent wholesale infrastructure provider, adheres to the principles of responsible corporate governance and provides high-quality telecommunications, technical, network and data centre infrastructure services for the operation of information and communications technology (ICT) and IT systems. Our aim is to ensure seamless and efficient service provision for our wholesale telecommunications partners and electronic communications service providers. **As an independent wholesale service provider, we uphold the principle of competitive neutrality in our operations and treat our partners equally and without discrimination.**

This Policy applies to all organisational units and employees of the Company, as well as to external service providers, suppliers and subcontractors acting on its behalf. It covers all personal data, information, systems, network and data centre components, processes and locations related to the provision of services.

Principles and Commitments

Taking into account the needs of stakeholders and changes in the operating environment, the Company ensures the protection of its partners' interests, as well as the rights and fundamental freedoms of natural persons. We are committed to

- processing personal data fairly, lawfully and transparently, and ensuring that data subjects can exercise their rights;
- maintain the confidentiality, integrity and availability of all information and system components;
- **treat business and technical information obtained from partners as confidential, do not make it available to other partners or third parties, and do not use it in a manner that undermines fair competition;**
- we prevent incidents that could jeopardise our services, minimise the risks they pose, and are prepared for their occurrence;
- we strengthen our partners' trust through the reliability and quality of our services.

The Company applies these principles as the foundation of its operations.

Compliance with legislation, standards and contracts

The Company complies with the legal and regulatory requirements applicable to its activities, in particular

- Regulation (EU) 2016/679 (GDPR) and Act CXII of 2011 on the right to data self-determination and freedom of information,
- Act LXIX of 2024 on Cyber Security in Hungary and its implementing regulations (in particular Government Decree 418/2024 (23 December)), as well as the requirements of Directive (EU) 2022/2555 (NIS2),
- the legislation in force relating to electronic communications, including provisions on the protection of communications secrecy and the security of services.

As a critical organisation, the Company cooperates with the Supervisory Authority for Regulated Activities (SZTFH), which is responsible for cyber security supervision; it fulfils its obligations regarding registration, notification and the payment of supervisory fees; and it regularly commissions the cyber security audit required by law.

We operate and develop our management systems in accordance with the ISO/IEC 27001:2022 and ISO 9001:2015 standards. We also fulfil our contractual and security obligations towards our partners.

Risk-based approach

The Company defines its data protection and information security requirements and controls in line with its business strategy, based on the results of risk management. The aim of the framework put in place is to support the secure operation of services, reduce risks and prevent incidents that could jeopardise the achievement of our objectives. Information security and quality management objectives are set annually by management and monitored using measurable indicators.

Key security areas

To ensure the security of its services, the Company establishes and maintains, in particular, the following:

- management and reporting of cyber security incidents in accordance with the applicable deadlines,
- business continuity and disaster recovery,
- vulnerability and change management,
- security of the supply and service chain,
- regular training and awareness-raising for employees,
- organisational and technical measures to protect personal data, including built-in and default data protection.

Responsibility and resources

The Company's senior management approves and oversees data protection and information security measures and assumes managerial responsibility for them. It provides the necessary resources, assigns areas of responsibility and authority, and ensures that the necessary policies, procedures and processes are documented and accessible to, and can be applied by, all those concerned. All employees and external contractors are obliged to comply with the Policy and the relevant regulations.

In line with **the need for continuous improvement,** the Company is committed to the ongoing enhancement of the effectiveness of its data protection, information security and quality management systems. This is based on internal audits, the findings of cyber security audits, management reviews, incident analysis and feedback from stakeholders.

The Company takes into account the impacts of climate change on its operations (e.g. the power supply and cooling of data centres, extreme weather events) and strives to reduce the environmental impact of its activities.

Publication and Review

The Policy is available to employees via an internal channel, to interested parties on request, or on the Company's website. It is reviewed annually by senior management, and whenever significant changes occur.

Budapest, 19 November 2026.

Gyöngyvér Papp-Gerlei, Chief Executive Officer