Business Continuity Policy

This document sets out the Business Continuity Policy adopted by **FiberCop S.P.A.**

FiberCop has implemented a Business Continuity Management System (**BCMS**) to safeguard the operation of its critical processes at an appropriate level in the event of incidents that may compromise service delivery, in line with the relevant methodologies and international standards, through:

- an **organizational structure** overseeing the implementation and management of its Business Continuity Management System, carrying out coordination, control, and methodological support activities for the operational and business functions to which the various processes and related supporting functions are assigned;
- **specific procedures** (the updating of which is guaranteed in line with contextual changes);
- the adoption of a **prevention model aligned with international standards**, which it maintains and improves to respond to evolving business needs and company processes. In particular, this operating model includes the following phases:
    I. identification and prioritization of the company's key processes;
    II. assessment of the business impacts resulting from the interruption of a process due to an event, incident, service disruption, or anomaly. In this phase, in addition to gathering general and contextual information about the process, the impacts on data confidentiality and integrity are analyzed (in terms of financial losses, management efficiency, reputational damage, and legal penalties), along with the maximum process recovery time (**Recovery Time Objective – RTO**), the maximum time between the last data backup and the occurrence of the event causing the process interruption (**Recovery Point Objective – RPO**), the

maximum period of process interruption beyond which the company's survival is compromised (**Maximum Tolerable Period of Disruption – MTPD**), the estimated financial losses if the process is unavailable, the critical suppliers supporting the process and their exclusivity, and the **Risk Assessment**, namely the identification, evaluation, and control of the risk level relating to the specific assets associated with each process (personnel, ICT systems, sites, and related facilities);

III. joint evaluation of the previous impact assessment phases and the Risk Assessment in order to determine whether it is necessary to prepare a **Business Continuity Plan – BCP** or introduce the actions required to reduce risk;

IV. drafting of the Business Continuity Plan, which describes effective Business Continuity solutions in terms of defining communication methods among interested parties and preparing the operating instructions to be executed for impact mitigation and process recovery. The Business Continuity Plan is intended to provide useful guidance for managing the following scenarios:

- *significant unavailability of ICT systems due to total or partial destruction of the site hosting them, inadequate functioning, or unavailability of the sites hosting them;*
- *unavailability of industrial sites or sites hosting personnel;*
- *significant unavailability of personnel due to voluntary or involuntary causes;*
- *significant unavailability of suppliers or of the products they provide;*
- *significant unavailability of core services provided to end customers;*

V. execution of tests of business continuity plans with the objective of both measuring performance, with possible reporting of remedial actions, and increasing the awareness of those responsible for acting to resolve or mitigate the effects of an adverse event;

- **awareness, training, and information programs** to promote the Business Continuity culture and the specific methods for managing operational disruptions, and to promote and disseminate principles and best practices with the aim of ensuring an effective Business Continuity Management System;
- the **monitoring of service disruptions and relevant events** from a continuous improvement perspective, supporting the evolution of existing continuity measures in order to promptly identify potential threats to the company and adopt the appropriate countermeasures;
- the **consolidation** and **expansion** of the **skills** required for the development and maintenance of its Business Continuity Management System;
- the **monitoring** of the **performance** of its Business Continuity program through specific KPIs.

As confirmation of the strategic importance attributed to Business Continuity, FiberCop has obtained **ISO 22301 certification**.