

## DESCRIPTION OF THE AVAILABILITY AND CAPACITY OF EU SOVEREIGN AND HIGHLY AVAILABLE TELECOMMUNICATIONS AND NETWORKING INFRASTRUCTURE WITH OPERATIONAL REDUNDANCY

Regarding point 14), namely “Description of the availability and capacity of EU sovereign and highly available telecommunications and networking infrastructure with operational redundancy”, it should be noted that the telecommunications and networking infrastructure planned for the identified site is designed to ensure maximum availability and operational resilience in accordance with the required security, reliability and service continuity requirements.

The backbone network architecture is based on a multi-layer, redundant and geographically distributed model, in order to ensure service continuity even in the event of localised faults and failures on individual nodes or backbones. All critical backbone components are implemented to ensure fault tolerance with automatic recovery.

The identified telecommunications operator is a legal entity of the European Union with full European control and governance, classified as an essential operator under the NIS2 Directive and subject to the corresponding security and oversight obligations.

### Features of Internet services offered and website resilience

Internet access will be redundant, with two independent and physically diverse fibre optic routes, with separate entry points to minimise the risk of single points of failure. Each access point will have redundant power supply and uninterruptible power supplies with a minimum autonomy of 72 hours in the event of a prolonged blackout.

The bandwidth planned for each link is at least 10Gbps, scalable to up to 100Gbps following structural network work.

Operational management is ensured by a **Network Operations Centre (NOC)** that is active **24 hours a day, 7 days a week, 365 days a year**, equipped with advanced proactive monitoring systems and automation tools that integrate artificial intelligence capabilities for the preventive detection of anomalies, congestion and critical issues in the network, ensuring high levels of continuity, operational resilience and service security. For essential services, a minimum availability of 99.99% on an annual basis is guaranteed, with maximum intervention and recovery times aligned with operational requirements.

### Network performance

Under normal conditions of use, the infrastructure outlined above ensures latencies of less than 5 ms to the European Internet Exchange Points MIX (Milan) and NaMeX (Rome) and average round-trip delays of less than 15 ms to the main OTT cloud platform<sup>1</sup> (AWS,

---

<sup>1</sup> OTT, which stands for ‘Over The Top’, refers to companies that provide services and content via the Internet without owning or directly managing the network infrastructure used for data transmission. In practice, OTTs offer platforms and

*Azure, Google Cloud, Oracle Cloud*) thanks to a direct interconnection with the Italian regions of these OTTs.

All backbone connections are managed using dynamic routing protocols, ensuring service continuity even in the event of planned maintenance or multiple faults.

### **Proximity to fibre optic backbones**

The operator's strategic sites, PoPs and main data centres are located close to the main national and international fibre optic backbones, with direct access to long-distance routes connecting the main European hubs and major OTTs.

This architecture allows the operator to offer low-latency, high-capacity connectivity services, as well as ensuring alternative routes between multiple directions to guarantee business continuity.

The provider is directly connected to multiple European Internet Exchange Points (IXPs), including MIX (Milan), NaMeX (Rome) and DE-CIX (Frankfurt), ensuring high redundancy and direct peering with major global operators and content providers.

The network can be connected via national providers, based on specific agreements, to supranational networks physically located within the European Union, in order to preserve the sovereignty of data transmission on the network.

This presence allows us to optimise routing paths and significantly reduce end-to-end latency to major public and private Internet services. Peering and routing policies are constantly optimised to ensure the best performance for cloud platforms and Italian public administration networks.

### **Operational redundancy and security**

Each critical component is managed with automatic failover mechanisms and geographical replication of network services (IP/MPLS). Infrastructure security is guaranteed by integrated *firewalling, DDoS protection, intrusion detection and traffic anomaly* analysis solutions, with ISO 27001 certification. Security and operational logs related to connectivity are stored in data centres located exclusively within the European Union, with a minimum retention period of 12 months and strictly controlled access.

The combination of multi-redundant architecture, widespread presence on optical backbones, direct connections to the main IXPs and proactive network management allows the provider not only to fully meet the indicators required by the tender, but to exceed them in terms of resilience, performance and operational security, offering a platform ready to support the future digital services of the European Public Administration. This implementation can also be replicated, with similar configurations, on a second provider to further increase the redundancy of the solution.

---

applications – such as cloud services (e.g. AWS, Azure, Google Cloud, Oracle Cloud), video streaming, messaging or social networks – that operate over the telecommunications networks provided by traditional operators, exploiting their connectivity to reach end users. The term “over the top” emphasises the fact that these services are delivered “above” the physical networks of telecommunications operators.