Additional Information Security Policies

Policy on Information Classification, Labeling, and Transfer (TISAX Point 1.3.2)
PSE establishes key principles for the classification, labeling, and handling of information in both electronic and paper format.

Policy on Information Security Incident Management (TISAX Point 1.6.1)
The purpose of this policy is to define the workflow for managing information security incidents within the PSE organization.

Policy on Mobile Devices and Teleworking (TISAX Point 2.1.4)
The purpose of this policy is to ensure adequate attention to the security of information and systems accessible via teleworking and mobile work, and to reduce the risk of security breaches occurring outside the usual workplace.
To protect data and information from illegal and/or harmful actions—whether intentional or unintentional—PSE adopts appropriate technical and organizational measures to prevent the loss, alteration, destruction, or damage of personal data and, more broadly, all company data and information.
PSE also trains its staff authorized for teleworking to ensure full understanding and compliance with relevant security procedures and policies.

Policy on Business Continuity Plan BCP and **Disaster Recovery Plan DRP** (TISAX Points 1.6.3 – 5.2.8 – 5.2.9)
In the context of PSE's operations, the internal delivery of Information and Communication Technologies (ICT) services is essential to the company's proper functioning, making it critical to ensure their business continuity.
For this reason, the company has implemented a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP) to provide procedures for managing and overcoming emergency and disaster situations that may disrupt normal service operations.

Access Control Policy (TISAX Point 4.1.2)
The purpose of this policy is to restrict access to information and information processing services and to prevent unauthorized access to systems and applications.

Password Management Policy (TISAX Point 4.1.3)
The purpose of this policy is to define how user authentication secrets (passwords) are managed.

Policy on the Use of Cryptographic Controls (TISAX Point 5.1.1)
PSE adopts systems to ensure the appropriate and effective use of cryptography to protect the confidentiality, authenticity, and/or integrity of information wherever necessary and/or feasible.

Information Transfer Policy (TISAX Point 5.1.2)
PSE adopts information transfer systems, supported by suitable tools, to preserve the integrity, confidentiality, and availability of information.

Change Management Policy (TISAX Point 5.2.1)
The purpose of this policy is to define how internal changes within PSE that may impact information security are managed and controlled.

Malware Protection Policy (TISAX Point 5.2.3)
The purpose of this policy is to ensure that information and information processing systems are protected against malware.

Technical Vulnerability Management Policy (TISAX Point 5.2.5)
The purpose of this policy is to prevent the exploitation of technical vulnerabilities.

Network Services Security Policy (TISAX Point 5.3.2)
The purpose of this policy is to ensure the protection of information within networks and the supporting information processing infrastructure.

PSE – Viale Umbria 4 – Grezzago (MI), Italy – Date: 25/02/2025

Management: PSE