egon
Address Quality

Information Security Policy

Egon S.r.l. considers the information that users entrust to or process through its services to be a valuable asset. For this reason, Egon S.r.l. assumes responsibility for protecting and enhancing this asset by ensuring that information is used with appropriate guarantees of accuracy and completeness and is adequately protected from misuse, unauthorized disclosure, damage, or loss.

This Information Security Policy reflects our commitment to safeguarding information through physical, logical, and organizational measures appropriate to all activities. It ensures the confidentiality, integrity, and availability of critical or sensitive entrusted information, with appropriate checks in place to prevent violations of these principles.

The objectives of the Information Security Policy are to:

1. Strengthen the company's reputation as a reliable and competent data manager;
2. Protect its information assets related to the Egon services platform and its associated services;
3. Gain a competitive advantage over other market players by emphasizing the value of information for Egon S.r.l.;
4. Minimize disruptions to users of the Egon services platform;
5. Adopt measures that foster staff loyalty and professionalism;
6. Fully comply with applicable and mandatory legislation;
7. Raise awareness and enhance staff competence regarding security issues;
8. Protect information from data loss by ensuring availability and integrity.

The objectives of the Cloud Services Policy are to:

1. Continuously assess the risks associated with privileged access by internal staff, ensuring authorizations are granted strictly based on operational needs and that activities are properly logged;
2. Guarantee data isolation for each customer by design, through logical segregation;
3. Implement control procedures for administrative access to cloud services;
4. Provide cloud service customers with advance email notifications regarding change management;
5. Ensure robust security for virtualization and the protection and access control of cloud service data;
6. Apply procedures for managing the lifecycle of cloud service customer accounts;
7. Ensure all security breaches are reported and that guidelines for information exchange with relevant authorities are followed.

Milan, 19/11/2024

The Management