ECO Certificazioni considera la sicurezza delle informazioni un elemento strategico, essenziale per la qualità dei servizi offerti e in coerenza con la propria mission aziendale.

L'organizzazione ha implementato un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), conforme alle normative vigenti, con l'obiettivo di proteggere dati aziendali e personali, garantendo **riservatezza**, **integrità** e **disponibilità** delle informazioni.

Principi fondamentali

- **Riservatezza**: accesso solo ad utenti e processi autorizzati.
- **Integrità:** protezione da modifiche non autorizzate o accidentali.
- **Disponibilità:** accesso sicuro e continuo ai dati autorizzati.
- **Controllo e autenticità:** uso di strumenti sicuri e tracciabilità delle informazioni.
- **Privacy:** trattamento dei dati personali conforme al GDPR.

Impegni dell'organizzazione:

- Progettazione "security by design" su infrastrutture e processi.
- Formazione e consapevolezza del personale e delle terze parti.
- Gestione tempestiva di anomalie e incidenti.
- Protezione fisica degli accessi e degli asset aziendali.
- Adozione di standard internazionali e rispetto normativo.
- Penetration test periodici per rilevare vulnerabilità.
- Assicurazione della business continuity e disaster recovery.

Responsabilità della Direzione

- Promuovere la cultura della sicurezza.
- Garantire affidabilità, efficienza e protezione dei processi e dei dati.
- Miglioramento continuo della politica tramite riesami periodici.
- Condivisione della policy con personale, terze parti e clienti.

La politica della sicurezza delle informazioni viene costantemente aggiornata e verificata, attraverso riesami periodici con le modalità e le tempistiche definite nella documentazione di sistema, per assicurare il suo continuo miglioramento ed è condivisa con l'organizzazione, le terze parti ed i clienti, attraverso la sua pubblicazione sul sito istituzionale aziendale.

ECO Certificazioni considers information security a strategic element, essential for the quality of the services provided and fully aligned with its corporate mission.

The organization has implemented an Information Security Management System (ISMS), compliant with applicable regulations, with the goal of protecting corporate and personal data while ensuring confidentiality, integrity, and availability of information.

Core Principles

- **Confidentiality**: information is accessible only to authorized users and processes.
- **Integrity**: protection against unauthorized or accidental modifications.
- **Availability**: secure and continuous access to authorized data.
- **Control and authenticity**: use of secure tools and traceability of information.
- **Privacy**: personal data processing in compliance with the GDPR.

Organizational Commitments

- "Security by design" in infrastructure and process development.
- Training and awareness for staff and third parties.
- Prompt management of anomalies and incidents.
- Physical protection of facilities and company assets.
- Adoption of international standards and legal compliance.
- Regular penetration testing to identify vulnerabilities.
- Assurance of business continuity and disaster recovery.

Management Responsibilities

- Promoting a security culture;
- Ensuring reliability, efficiency, and protection of processes and data;
- Continuous improvement of the policy through periodic reviews.
- Sharing the policy with staff, third parties, and clients.

The Information Security Policy is regularly updated and reviewed through periodic assessments, according to the methods and timelines defined in the system documentation, to ensure its continual improvement. It is shared with the organization, third parties, and clients through its publication on the company's official website.

Faenza, 13/06/2025

F.to dott.ssa Serena Farina

Presidente del Consiglio di Amministrazione