

Politica per la sicurezza delle informazioni

FULL SERVICE SOLUTION S.R.L. eroga servizi di collaudo, installazione, assistenza tecnica e consulenza relativi ad apparati hardware e software. Nello svolgimento di queste attività accede quotidianamente ai sistemi, alle configurazioni e ai dati dei propri Clienti, opera presso le loro sedi e riceve in custodia credenziali, apparati e informazioni riservate. Da questa posizione discende una responsabilità che la Direzione considera parte integrante del servizio e non un adempimento accessorio: la fiducia che il Cliente ripone nell'organizzazione quando le apre l'accesso ai propri sistemi è essa stessa il bene da proteggere.

1. Scopo e campo di applicazione

Con la presente Politica l'Amministratore Unico stabilisce gli indirizzi in materia di sicurezza delle informazioni, definisce il quadro di riferimento per gli obiettivi e assume gli impegni che governano il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), conforme alla norma UNI CEI ISO/IEC 27001:2022 e al relativo Emendamento 1:2024.

La Politica si applica all'intero campo di applicazione del SGSI: «Erogazione di servizi di collaudo, installazione, assistenza tecnica e consulenza relativi ad apparati hardware e software», a tutto il personale e alle parti esterne che accedono alle informazioni dell'organizzazione o dei Clienti.

2. Impegni della Direzione

L'Amministratore Unico si impegna a:

- a) **Soddisfare i requisiti applicabili:** requisiti di legge (in particolare il GDPR e il Provvedimento del Garante sugli Amministratori di Sistema), contrattuali verso Clienti e fornitori, e quelli derivanti dall'analisi del contesto e delle parti interessate;
- b) **Migliorare continuamente il SGSI:** attraverso la valutazione dei rischi, l'analisi degli incidenti, gli audit, il Riesame della Direzione e le azioni correttive e di miglioramento registrate in FS_PM_001;
- c) **Mettere a disposizione le risorse necessarie** e assicurare che ruoli e responsabilità siano assegnati e conosciuti.

3. Quadro di riferimento per gli obiettivi

La presente Politica costituisce il quadro di riferimento per gli obiettivi per la sicurezza delle informazioni, stabiliti nel documento FS_Ob_001, misurabili, coerenti con la valutazione dei rischi e riesaminati almeno una volta l'anno. Gli indirizzi generali sono:

- proteggere la riservatezza delle informazioni e dei sistemi dei Clienti durante tutti gli interventi;
- assicurare l'integrità e la tracciabilità delle attività svolte sui sistemi dei Clienti;
- garantire la disponibilità dei servizi di assistenza, anche in caso di eventi avversi;
- mantenere il personale formato e consapevole delle proprie responsabilità;
- gestire gli incidenti in modo tempestivo, limitandone l'impatto e traendone insegnamento.

4. Principi

- **Riservatezza, integrità e disponibilità:** le informazioni sono accessibili solo a chi è autorizzato, sono accurate e complete e sono disponibili quando servono.
- **Gestione dei rischi:** i rischi sono identificati, valutati e trattati in modo sistematico secondo la metodologia del documento FS_RA_001, per mantenerli a un livello accettabile.
- **Rispetto dei sistemi dei Clienti:** l'accesso ai sistemi dei Clienti avviene solo se autorizzato, con strumenti approvati e in modo tracciato; le credenziali di sessione dei Clienti non sono conservate; i dati dei Clienti non sono copiati senza autorizzazione; gli apparati sono resettati prima della riconsegna e i supporti sostituiti sono distrutti.
- **Fornitori:** i fornitori che trattano informazioni per conto dell'organizzazione sono vincolati a requisiti di sicurezza adeguati.
- **Competenza e consapevolezza:** il personale è verificato all'inserimento, formato e periodicamente aggiornato.
- **Cambiamento climatico:** in conformità all'Emendamento 1:2024, il cambiamento climatico è considerato tra i fattori del contesto per i suoi effetti sulla continuità e sulla disponibilità dei servizi.

5. Ruoli e responsabilità

- **Amministratore Unico:** è il responsabile ultimo del SGSI; approva la Politica, gli obiettivi e l'accettazione dei rischi residui.
- **Responsabile del Sistema di Gestione (RSG):** coordina le attività del SGSI, ne monitora l'efficacia e propone i miglioramenti.
- **Amministratore di Sistema interno:** gestisce in sicurezza i sistemi e i servizi informatici aziendali.
- **Tutto il personale:** ogni dipendente, collaboratore e parte esterna rispetta la Politica e le procedure correlate e segnala tempestivamente al RSG ogni evento o incidente, anche solo sospetto.

6. Gestione degli incidenti

Gli eventi e gli incidenti di sicurezza sono segnalati al RSG e gestiti secondo le procedure FS_Gestione_Commissa_1 e FS_PDB_001, con l'obiettivo di limitarne l'impatto, informare i Clienti coinvolti e prevenirne il ripetersi.

7. Comunicazione e riesame

La Politica è comunicata a tutto il personale all'inserimento e durante la formazione annuale, è pubblicata sul sito internet aziendale ed è resa disponibile alle parti interessate che ne fanno richiesta. È riesaminata dall'Amministratore Unico almeno una volta l'anno, in occasione del Riesame della Direzione, o in caso di cambiamenti significativi del contesto, dei servizi o della normativa.

Roma 06.09.2026

FULL SERVICE SOLUTION S.R.L.
L'Amministratore Unico