Consulting Service ®

POLITICA INTEGRATA

Qualità – Ambiente – Salute e Sicurezza sul Lavoro – Sicurezza delle Informazioni

PREMESSA

La **CONSULTING SERVICE S.r.l.** intende perseguire l'obiettivo di fornire servizi sempre più rispondenti ai bisogni e alle aspettative dei propri clienti. Per continuare a essere un'azienda sana e competitiva, in un mercato dinamico e in costante cambiamento, è indispensabile sviluppare servizi che offrano ai clienti un prodotto finale di valore e qualità. L'obiettivo è trasformare nel tempo l'azienda affinché i servizi diventino il fulcro della mission aziendale.

Con l'avvento delle nuove tecnologie e dei software per i modelli di Industria 4.0, Consulting Service pone l'accento su soluzioni che integrano e automatizzano i processi interni ed esterni, proponendo software di digitalizzazione e strumenti avanzati per restare un interlocutore unico in linea con i nuovi trend. Poiché tali servizi comportano la gestione di sistemi, reti, dati e documenti propri e dei clienti, **la sicurezza delle informazioni è parte integrante della qualità del servizio** e della fiducia che i clienti ripongono nell'azienda.

Alla luce di una diversa coscienza sociale, l'azienda intende inoltre migliorare le prestazioni ambientali, valutando il rispetto dell'ambiente non solo come valore etico ma come occasione per soddisfare nuovi bisogni, e incrementare la tutela della salute e della sicurezza dei propri dipendenti e clienti. Propone alla clientela soluzioni *total green*, in grado di realizzare concreti vantaggi ambientali ed economici, e a fronte dell'installazione delle apparecchiature acquista "bonus green" per limitare l'emissione di CO_2 da esse prodotta.

La presente Politica Integrata si applica al Sistema di Gestione Integrato conforme a UNI EN ISO 9001:2015, UNI EN ISO 14001:2015, UNI ISO 45001:2018 e **UNI CEI EN ISO/IEC 27001:2024** (ISO/IEC 27001:2022 e relativo Amendment 1:2024), e costituisce la politica per la sicurezza delle informazioni di cui al punto 5.2 della norma e al controllo 5.1 dell'Annex A. Il campo di applicazione del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) è: *Consulenza, progettazione, vendita, assistenza, manutenzione di infrastrutture IT, servizi cloud, servizi cybersecurity, fornitura HW e software di terze parti*.

IMPEGNI DELLA DIREZIONE

La Direzione si impegna ad applicare in prima persona le regole stabilite nel Manuale Integrato e nelle procedure in esso richiamate e a verificarne l'applicazione da parte di tutto il personale. Il modello di governance adottato include obiettivi definiti in modo chiaro e un processo di controllo che ne assicura il rispetto. In particolare, la Direzione si impegna a:

- soddisfare i requisiti applicabili: cogenti (tra cui il Regolamento (UE) 2016/679 – GDPR, il D.Lgs. 196/2003 e s.m.i., il D.Lgs. 81/2008 e la normativa ambientale), contrattuali e delle parti interessate, compresi gli accordi di riservatezza e i livelli di servizio concordati con i clienti;
- prevenire impatti negativi sull'ambiente e sulla salute, ridurre rifiuti ed emissioni e garantire condizioni di lavoro sicure e salubri, eliminando i pericoli e riducendo i rischi per la salute e sicurezza, con la consultazione e partecipazione dei lavoratori;
- proteggere le informazioni proprie, dei clienti e dei partner da accessi non autorizzati, perdita, alterazione o indisponibilità, sulla base di una valutazione e trattamento dei rischi periodica e documentata;
- assicurare le risorse necessarie (persone, competenze, infrastrutture e strumenti tecnologici) per il funzionamento efficace del Sistema di Gestione Integrato;
- perseguire il **miglioramento continuo** del Sistema di Gestione Integrato e delle prestazioni in materia di qualità, ambiente, salute e sicurezza e sicurezza delle informazioni.

POLITICA INTEGRATA

Qualità – Ambiente – Salute e Sicurezza sul Lavoro – Sicurezza delle Informazioni

PRINCIPI PER LA SICUREZZA DELLE INFORMAZIONI

Consulting Service considera le informazioni un patrimonio aziendale e le tutela lungo tutto il loro ciclo di vita, in qualsiasi forma (cartacea, digitale, verbale) e su qualsiasi supporto, secondo tre principi fondamentali:

Principio	Significato per Consulting Service
Riservatezza	Le informazioni aziendali, dei clienti e i dati personali sono accessibili solo a chi è autorizzato, in base al principio del "need to know" e del minimo privilegio.
Integrità	Le informazioni e le configurazioni gestite (sistemi, reti, documenti nel gestionale ADIUTO) sono accurate, complete e modificate solo da personale autorizzato e tracciato.
Disponibilità	Servizi, sistemi e dati sono accessibili quando necessario, anche per l'assistenza ai clienti, grazie a backup, ridondanza e gestione della continuità operativa.

Per tradurre questi principi in pratica, l'azienda adotta i seguenti criteri:

- **approccio basato sul rischio**: i rischi per la sicurezza delle informazioni sono identificati, valutati e trattati secondo una metodologia documentata, con criteri di accettazione approvati dalla Direzione; i controlli dell'Annex A sono selezionati e motivati nella Dichiarazione di Applicabilità;
- **gestione degli asset**: gli asset informativi (hardware, software, dati, servizi cloud) sono inventariati, classificati e assegnati a un responsabile;
- **controllo degli accessi**: credenziali personali, autenticazione forte per gli accessi critici e remoti, revoca tempestiva dei privilegi al cambio di ruolo o cessazione;
- **sicurezza nei rapporti con fornitori e partner tecnologici**: requisiti di sicurezza e riservatezza nei contratti e verifica periodica dei fornitori critici, inclusi i servizi cloud;
- **sicurezza presso i clienti**: le attività di installazione, configurazione e assistenza remota sui sistemi dei clienti sono svolte con procedure controllate e nel rispetto delle loro regole di sicurezza;
- **gestione degli incidenti**: ogni evento o debolezza di sicurezza va segnalato tempestivamente, gestito e analizzato per prevenirne il ripetersi, adempiendo agli obblighi di notifica previsti (es. violazioni di dati personali);
- **continuità operativa**: backup verificati e piani di ripristino per garantire la continuità dei servizi critici.

OBIETTIVI

In funzione di quanto esposto per la qualità, l'ambiente, la salute e sicurezza e la sicurezza delle informazioni, la Direzione si impegna a perseguire i seguenti obiettivi, declinati annualmente in traguardi misurabili, con responsabili, risorse e scadenze, monitorati e riesaminati in sede di Riesame della Direzione:

- Orientare l'organizzazione all'ampliamento del portafoglio Clienti al fine di incrementare la redditività dell'impresa.
- Fidelizzare il Cliente attraverso la stipula di contratti di manutenzione, assistenza tecnica e noleggio.
- Identificare le esigenze e le aspettative del Cliente in modo da poterlo soddisfare, comprese quelle relative alla protezione dei suoi dati e sistemi.
- Mantenere le certificazioni dei propri sistemi in conformità a UNI EN ISO 9001:2015, UNI EN ISO 14001:2015 e UNI ISO 45001:2018 e conseguire e mantenere la certificazione UNI CEI EN ISO/IEC 27001.
- Garantire la riservatezza, l'integrità e la disponibilità delle informazioni aziendali e dei clienti, riducendo il numero e l'impatto degli incidenti di sicurezza.

POLITICA INTEGRATA

Qualità – Ambiente – Salute e Sicurezza sul Lavoro – Sicurezza delle Informazioni

- Mantenere aggiornate la valutazione dei rischi per la sicurezza delle informazioni e la Dichiarazione di Applicabilità, adeguandole all'evoluzione di minacce, tecnologie, servizi offerti e contesto (inclusi gli effetti dei cambiamenti climatici, ove rilevanti).
- Proteggere infrastrutture, postazioni e servizi cloud mediante aggiornamenti tempestivi, protezione da malware, backup verificati e monitoraggio delle vulnerabilità.
- Diffondere tali politiche sia **all'interno** dell'azienda, coinvolgendo tutto il personale per il raggiungimento dei traguardi prestabiliti mediante riunioni e reporting periodici, sia **all'esterno**, attraverso un flyer informativo, la pubblicazione sul sito web, la presentazione aziendale, la modulistica recante i loghi degli Enti di certificazione, la pubblicità tramite jumbo screen nei comuni limitrofi e l'affissione in bacheca presso l'ufficio, insieme all'organigramma.
- Operare per il continuo coinvolgimento del personale e per lo sviluppo delle competenze, mediante momenti di formazione e informazione, perseguendo la crescita, la consapevolezza e il senso di responsabilità di tutti i collaboratori, e garantire un alto livello di professionalità a livello manageriale, gestionale e operativo.
- Sensibilizzare tutto il personale sulle problematiche ambientali, di sicurezza sul lavoro, di sicurezza delle informazioni ed etiche, con piani di formazione periodici (es. phishing, gestione password, uso corretto dei dispositivi e dei dati dei clienti), sottolineando l'importanza del contributo di ciascuno al miglioramento delle condizioni di sicurezza, dell'efficienza ambientale e degli standard qualitativi.
- Valutare e controllare gli impatti ambientali delle attività, incrementando il livello tecnologico di apparecchiature, macchinari e attrezzature e riducendo consumi energetici, consumo di carburante ed emissioni in atmosfera, incoraggiando la raccolta e il riciclo dei prodotti a fine vita.
- Mantenere un sistema di informazione, formazione e aggiornamento costante rispetto all'evoluzione dei prodotti disponibili sul mercato.
- Privilegiare fornitori che garantiscano materiali, parti e prodotti a ridotto impatto ambientale e adeguati livelli di sicurezza delle informazioni.
- Gestire l'archiviazione informatica dei documenti tramite il documentale ADIUTO, assicurando controllo degli accessi, tracciabilità, conservazione e salvataggio dei dati.
- Garantire la dismissione sicura di apparecchiature e supporti (cancellazione certificata dei dati da stampanti multifunzione, PC e dispositivi ritirati da clienti o a fine noleggio), in coerenza con l'obiettivo di economia circolare.
- Creare un'economia circolare relativa ai materiali di scarto e di imballaggio.

COMUNICAZIONE, RESPONSABILITÀ E RIESAME

La presente politica è mantenuta come informazione documentata, comunicata a tutto il personale e ai collaboratori, resa disponibile alle parti interessate e supportata da politiche specifiche per tema (es. uso accettabile degli strumenti ICT, controllo accessi, backup, gestione incidenti, rapporti con i fornitori, lavoro da remoto).

Tutto il personale e i collaboratori sono tenuti a rispettarla; le violazioni sono gestite secondo il sistema disciplinare aziendale. La Direzione individua un Responsabile del Sistema di Gestione Integrato, con autorità e responsabilità anche per la sicurezza delle informazioni riportato in organigramma.

La politica è riesaminata almeno annualmente, e comunque in caso di cambiamenti significativi del contesto, dei servizi o dei rischi, per accertarne l'adeguatezza e la coerenza con le strategie aziendali e con lo sviluppo dei sistemi di gestione per la qualità, l'ambiente, la salute e sicurezza sul lavoro e la sicurezza delle informazioni.

Palestrina, lì *01/07/2026*

La Direzione

