POLITICA QUALITA', AMBIENTE E SICUREZZA DELLE INFORMAZIONI

IL Gruppo S.P.E., di seguito S.P.E., si occupa dello sviluppo, della fornitura e del mantenimento dei servizi di telecomunicazione di rete fissa, della progettazione e sviluppo software e della fornitura di servizi per la conservazione di documenti informatici, impegnandosi a soddisfare le esigenze esplicite ed implicite dei Clienti assicurando l'affidabilità e la qualità dei servizi e dei prodotti offerti, nel pieno rispetto delle prescrizioni legali e dei regolamenti.

In particolare, S.P.E. offre ai propri Clienti servizi cloud per la gestione e l'utilizzo di programmi e applicativi connessi ai software sviluppati e servizi per la fornitura di spazio web e l'archiviazione dei dati (Servzi SaaS, Paas, IaaS) con possibilità di effettuare la conservazione sostitutiva di documenti informatici.

La Direzione di S.P.E. ha definito una specifica Politica di Sicurezza delle Informazioni (Information Security Policy Document - ISPD) cui si rimanda per la definizione dei principi per le attività di Conservatore di documenti informatici.

Per fornire prodotti e servizi innovativi ed efficienti, S.P.E. nel tempo si è adeguatamente strutturata, per questo motivo ha deciso di adottare un Sistema di Gestione per la Qualità conforme alla norma UNI EN ISO 9001:2015, un Sistema di Gestione Ambientale conforme alla norma UNI EN ISO 14001:2015 e un Sistema di Gestione Integrato per la Sicurezza delle Informazioni (SGSI), in conformità alle norme UNI CEI EN ISO/IEC 27001: 2024, UNI CEI EN ISO/IEC 27002: 2023, UNI CEI EN ISO/IEC 27017: 2021, UNI CEI EN ISO/IEC 27018: 2020, ISO 14721:2012, ISO/IEC 15489-1:2016, ETSI EN 319 401 V3.1.1 (2024-06), ETSI TS 119 511 V1.1.1 (2019-06).

Nel quadro dell'impegno verso l'attuazione della Politica per la sicurezza delle informazioni, S.P.E. persegue i propri obiettivi tenendo conto dei seguenti valori di riferimento:

- la soddisfazione del Cliente, quale elemento centrale per l'organizzazione;
- la creazione di Valore, attraverso l'innovazione tecnologica ed il miglioramento continuo dei processi, perseguendo efficacia ed efficienza come condizioni prioritarie per la crescita competitiva e per il raggiungimento della leadership tecnologica e di mercato;
- il rispetto delle regole e dei requisiti applicabili, nonché dei principi etici di trasparenza e correttezza;
- la coerenza con i livelli di rischio accettabili per le informazioni trattate nei servizi cloud e negli altri asset.

La Direzione Generale di S.P.E., attraverso un'evoluzione organizzativa focalizzata ed integrata, stabilisce e riesamina i propri obiettivi volti in particolare a:

- sviluppare servizi accurati e di qualità, soddisfacendo le attese dei Clienti;
- sviluppare le architetture e le piattaforme delle reti di telecomunicazioni fisse, a garanzia della copertura e dell'accessibilità ai servizi e adottando tecnologie all'avanguardia;
- sviluppare prodotti e software in base alle specifiche richieste del Cliente;
- custodire e valorizzare i propri asset adottando strategie di ottimizzazione e di progressivo rinnovamento;
- valorizzare la competenza, la professionalità e la responsabilizzazione delle proprie risorse umane promuovendo tutte le possibili sinergie, sostenendo altresì la tutela dell'ambiente e della salute e sicurezza nei luoghi di lavoro;
- assicurare il miglioramento continuo dei processi end-to-end, in termini di efficacia e di efficienza.

Lo strumento operativo adottato da S.P.E. a sostegno della Politica e del quadro di riferimento degli obiettivi sopra descritti è costituito dal Sistema di Gestione Integrato della Qualità, Ambiente e Sicurezza delle Informazioni (SGSI).

La gestione della Sicurezza delle informazioni è una priorità aziendale, che attribuisce importanza strategica al trattamento delle informazioni e concretizza la volontà di difendere la confidenzialità, l'integrità e la disponibilità dei dati.

Gli obiettivi principali del SGSI si realizzano nell'assicurare:

- La **riservatezza** del patrimonio informativo gestito: proprietà per cui l'informazione non è resa disponibile o comunicata a individui, entità o processi non autorizzati;
- L'**integrità** del patrimonio informativo gestito: proprietà di tutelare l'accuratezza e la completezza degli asset, ossia di qualsiasi informazione o bene attinente a cui l'organizzazione attribuisce un valore;
- La **disponibilità** del patrimonio informativo gestito: proprietà per cui l'informazione deve essere accessibile ed utilizzabile previa richiesta di una entità autorizzata;
- **L'autenticità** le informazioni devono essere mantenute originali in riferimento alla validità e conformità delle stesse;
- L'ottemperanza ai **requisiti cogenti**, normativi e contrattuali;
- La redazione di piani per la continuità dell'attività aziendale che siano costantemente aggiornati e controllati;
- L'adeguata **formazione** in tema di sicurezza delle informazioni del personale;
- La corretta gestione di tutte le **violazioni** della sicurezza delle informazioni e dei possibili punti deboli, al fine di una corretta rilevazione ed indagine.

S.P.E., al fine di migliorare la resilienza e il livello complessivo di sicurezza informatica ha provveduto ad attuare quanto previsto dalla Direttiva NIS 2 - Direttiva UE 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 e dal decreto di recepimento il D.Lgs. 4 settembre 2024, n. 138.

In particolare, S.P.E. con l'applicazione dei principi NIS 2 vuole rafforzare la propria resilienza alle minacce informatiche, provvedendo a migliorare le proprie modalità operative per:

- identificare, valutare e mitigare i rischi di cybersecurity;
- valutare proattivamente le prestazioni di cybersecurity;
- gestire la continuità operativa dell'Organizzazione;
- la definizione di compiti e responsabilità dei collaboratori;
- formare costantemente i collaboratori migliorandone la consapevolezza per la cybersecurity;
- rafforzare le difese organizzative e tecnologiche;
- gestire le identità, l'autenticazione e il controllo degli accessi;
- la gestione degli asset;
- monitorare costantemente gli accessi ai propri sistemi;
- controllare la catena di fornitura;
- gestire e segnalare gli incidenti;
- definire piani di risposta agli incidenti;
- attuare adeguati piani di ripristino dagli incidenti.

S.P.E. ha sviluppato le misure di cybersecurity considerando quanto specificato anche dal Framework nazionale per la Cybersecurity e la Data Protection, best practice internazionali di riferimento per la normativa di settore.

Nel corso dell'anno 2024, al fine di migliorare le proprie prestazioni ambientali S.P.E. ha deciso di implementare un modello di gestione conforme alla norma UNI EN ISO 14001:2015.

La visione ed i valori essenziali di S.P.E. per l'Ambiente sono così riassumibili:

- il rispetto per l'Ambiente e il contenimento delle emissioni di CO2 è fondamentale ed irrinunciabile per ogni attività operativa aziendale;
- il rispetto della legislazione vigente e dei requisiti sottoscritti è imprescindibile da qualsiasi altra considerazione;
- l'attenzione all'Ambiente è intesa come attività di prevenzione generale e non solo come insieme di interventi correttivi per l'eliminazione delle Non Conformità rilevate o semplice adeguamento legislativo;
- la gestione degli aspetti legati al cambiamento climatico è considerata con particolare attenzione dalla Direzione aziendale che si impegna a ridurre gli impatti che le attività aziendali possono avere sul clima;
- la responsabilità di applicazione del SGI è in carico a ciascun operatore secondo le proprie attribuzioni e competenze.

Applicabilità.

Tutti i collaboratori e i fornitori coinvolti nell'applicazione del Sistema di gestione Qualità, Ambiente e Sicurezza delle Informazioni sono responsabili dell'attuazione della presente Politica aziendale con il supporto della Direzione Generale che ha approvato la Politica stessa.

Responsabilità.

Il Responsabile Qualità, Ambiente e Sicurezza delle informazioni facilita l'attuazione della presente Politica attraverso norme e procedure appropriate.

Tutti i collaboratori sono tenuti a rispettare quanto indicato specificatamente dalle Regole di Comportamento aziendali controfirmate al momento dell'inizio del rapporto di collaborazione con S.P.E..

Tutti i collaboratori devono seguire le procedure stabilite da S.P.E. e i principi enunciati nella Politica Qualità, Ambiente e Sicurezza delle informazioni, applicando per le parti di competenza tutti i controlli previsti dalla SOA aziendale e dal SGSI.

Tutti i collaboratori, in base alle proprie conoscenze, hanno la responsabilità di riferire al Responsabile Qualità, Ambiente e Sicurezza delle informazioni qualsiasi punto debole individuato.

Traguardi.

La Direzione generale di S.P.E. vuole:

- Identificare una metodologia di valutazione del rischio adeguata al Sistema di Gestione Qualità, Ambiente e Sicurezza delle informazioni, ai requisiti di business individuati, a quelli cogenti e normativi;
- Preservare attraverso, un'adeguata analisi dei rischi e delle opportunità, il valore del patrimonio informativo, all'interno del campo di applicazione del Sistema di Gestione Qualità, Ambiente e Sicurezza delle informazioni, al fine di comprendere le vulnerabilità e le possibili minacce che possano esporlo a rischio;
- Gestire il rischio ad un livello accettabile e allinearlo al più generale contesto di gestione del rischio strategico dell'organizzazione;
- Definire e rendere effettive le linee operative per una architettura di sicurezza intesa come l'insieme di regole, funzioni, strumenti, oggetti e controlli, coerentemente disegnati e resi funzionanti, che garantiscano in ogni struttura organizzativa, ambiente informatico, singolo elaboratore, il rispetto degli standard definiti dall'azienda;
- Controllare, cogliendo ogni spunto di miglioramento, il Sistema di gestione attuato.

Nell'ambito dell'erogazione dei servizi cloud, S.P.E. si configura come Cloud Service Providers (CSP) o Data Processor delle PII nel cloud pubblico per i propri clienti e come Cloud Service Customers (CSC) per le attività assegnate ai propri fornitori del servizio cloud.

S.P.E. si impegna a rispettare la legislazione cogente applicabile in materia di protezione dei dati personali (PII) e le condizioni contrattuali concordate tra il Data Processor delle PII nel cloud pubblico e i CSC, applicando le disposizioni previste dal Regolamento UE 679/20016 e dal D.Lgs. 196/2003 e s.m.i..

Politica per la sicurezza delle informazioni nei servizi cloud per il CSP

S.P.E. ha provveduto a disciplinare la fornitura e l'uso dei servizi cloud, considerando:

- i requisiti sulla sicurezza applicabili su cui si basa la progettazione e l'implementazione del servizio cloud;
- i rischi derivati dagli accessi degli addetti interni autorizzati;
- l'isolamento degli accessi dei diversi utenti CSC ai servizi multiutente;
- l'accesso alle informazioni del CSC da parte del personale del CSP;
- la definizione delle procedure di controllo degli accessi, con particolare riferimento all'autenticazione forte per gli accessi amministrativi ai servizi cloud;
- la comunicazione ai CSC durante la gestione dei cambiamenti;
- gli aspetti di sicurezza della virtualizzazione;
- l'accesso e protezione dei dati dei CSC;
- la gestione del ciclo di vita dell'account del CSC;
- la comunicazione delle violazioni dei dati (data breaches) e condivisione delle linee guida per aiutare le investigazioni e indagini giudiziarie.

Politica per la sicurezza delle informazioni nei servizi cloud per il CSC

Quando S.P.E. utilizza servizi come Cloud Service Customers (CSC) verifica attentamente le modalità con le quali:

- le informazioni archiviate nell'ambiente cloud sono soggette ad accesso e gestione da parte del CSP;
- le risorse sono mantenute nell'ambiente cloud (es. programmi applicativi);
- i processi sono eseguiti su un servizio cloud virtualizzato multiutente;
- viene identificato l'utente che utilizza il servizio cloud e il contesto nel quale può utilizzarlo;
- viene definito chi è l'amministratore di sistema e la tipologia di privilegi di accesso assegnati;
- è definita la localizzazione geografica del CSP e il paese dove sono conservati i dati del servizio cloud.

La presente Politica del Sistema di gestione Integrato deve essere riesaminata periodicamente e tutte le volte che intervengano modifiche all'organizzazione o al Sistema di gestione implementato, per assicurare che permanga idonea alle esigenze Aziendali e alle aspettative del Cliente e di tutte le parti interessate.

Brescia, 14 gennaio 2026

La Direzione Generale

Paolo Prandini