INDICE

MATRICE DELLE REVISIONI					
REVISIONE	DATA	DESCRIZIONE / SEGNALAZIONE TIPO MODIFICA	REDATTA: RSI	VERIFICATA: RSI	APPROVATA: DIR
01	24.09.2024	prima emissione	***PAOLO PRANDINI***	***PAOLO PRANDINI***	***PAOLO PRANDINI***

LISTA DI DISTRIBUZIONE				
COPIA CONTROLLATA N°	FUNZIONE	NOMINATIVO DEL RICEVENTE	DATA CONSEGNA	FIRMA RICEVENTE
1	DIR	24.09.2024	***PAOLO PRANDINI***	***PAOLO PRANDINI***
1	RSI	24.09.2024	***PAOLO PRANDINI***	***PAOLO PRANDINI***

0. INTRODUZIONE

Il documento di Politica di Sicurezza delle Informazioni (Information Security Policy Document - ISPD) per le attività di Conservatore definisce le Politiche adottate da SPE.IT S.r.l., di seguito indicata semplicemente come SPE.IT, per assicurare la corretta gestione della Sicurezza delle informazioni e tutelare le informazioni documentate conservate a qualunque titolo nel proprio sistema informativo.

Il presente documento è considerato “Pubblico” in quanto contiene informazioni che possono essere comunicate liberamente senza che vi possano essere conseguenze negative per SPE.IT o i terzi interessati; è consultabile all'indirizzo: www.spe.it.

SPE.IT definisce la riservatezza dei documenti trattati nel rispetto della seguente casistica:

Tipologia di documento		
Pubblico	**Interno**	**Riservato**
Il documento può essere diffuso all'esterno dell’Organizzazione. Le informazioni sono accessibili a chiunque, la divulgazione non provoca danni.	Il documento può essere diffuso solo all'interno dell’Organizzazione. Le informazioni sono accessibili a tutto il personale, la divulgazione crea minori disagi o minori inconvenienti organizzativi. Le terze parti a cui viene comunicato, hanno l’obbligo di non diffonderlo.	Il documento non può essere diffuso all'interno dell’Organizzazione e rimane visibile ai soli interessati alla gestione dello stesso. L’accesso alle informazioni è pertanto riservato al personale interno in base alle specifiche autorizzazioni di DIR, la divulgazione ha un impatto significativo a breve termine nelle operazioni o obiettivi tecnici. L'indicazione “Riservato” deve essere chiaramente riportata nel documento.

1. SCOPO E CAMPO DI APPLICAZIONE

Scopo del Documento sulla Politica di Sicurezza delle Informazioni per le attività di Conservatore è descrivere i principi fondamentali applicati con il Sistema di Gestione per la Sicurezza delle Informazioni implementato da SPE.IT.

SPE.IT considera le informazioni gestite, per il particolare rilievo che hanno assunto, parte integrante del proprio patrimonio. È obiettivo di assoluta priorità per SPE.IT, salvaguardare la sicurezza del proprio sistema informativo e tutelare la riservatezza, l’integrità e la disponibilità delle informazioni prodotte, raccolte o comunque trattate, da ogni minaccia intenzionale o accidentale, interna o esterna.

SPE.IT si impegna a implementare e mantenere attivo il Sistema di Gestione per la Sicurezza delle Informazioni per garantire la corretta gestione delle risorse informative fisiche e logiche nel pieno rispetto dei requisiti cogenti, di erogazione del servizio e contrattuali.

La Politica di Sicurezza delle Informazioni si applica a tutte le informazioni trattate da SPE.IT, con l’applicazione del Sistema di Gestione per la Sicurezza delle Informazioni da parte dei collaboratori interni ed esterni e, dai terzi che, a vario titolo, fruiscono dei servizi offerti dall’Organizzazione.

Il campo di applicazione del Sistema di Gestione per la Sicurezza delle Informazioni per le attività di Conservatore è:

Scopo del Gruppo S.P.E.

UNI CEI EN ISO/IEC 27001:2024: Erogazione di servizi di telecomunicazione, di progettazione e sviluppo software e di servizi di Cloud Computing, in modalità IaaS – PaaS – SaaS, con l'utilizzo delle Linee guida UNI CEI EN ISO/IEC 27017 e UNI CEI EN ISO/IEC 27018.

Erogazione del servizio di conservazione di documenti informatici.

SoA rev. 00 del 24/09/2024.

UNI EN ISO 9001:2015 e UNI EN ISO 14001:2015: Erogazione di servizi di telecomunicazione, di progettazione e sviluppo software e di servizi di Cloud Computing, in modalità SaaS. Erogazione del servizio di conservazione di documenti informatici.

Assistenza tecnica e supporto alla Pubblica amministrazione per i servizi in Cloud (IaaS – PaaS – SaaS).

S.P.E. Sistemi e Progetti Elettronici S.a.s. di Prandini Paolo e C.

UNI CEI EN ISO/IEC 27001:2024: Erogazione di servizi di telecomunicazione, di progettazione e sviluppo software e di servizi di Cloud Computing, in modalità IaaS – PaaS – SaaS, con l'utilizzo delle Linee guida UNI CEI EN ISO/IEC 27017 e UNI CEI EN ISO/IEC 27018. SoA rev. 00 del 24/09/2024.

UNI EN ISO 9001:2015 e UNI EN ISO 14001:2015: Erogazione di servizi di telecomunicazione, di progettazione e sviluppo software e di servizi di Cloud Computing.

Assistenza tecnica e supporto alla Pubblica amministrazione per i servizi in Cloud (IaaS – PaaS – SaaS).

SPE.IT s.r.l. a socio unico

UNI CEI EN ISO/IEC 27001:2024: Erogazione di servizi di progettazione e sviluppo software e di servizi di Cloud Computing, in modalità SaaS, con l'utilizzo delle Linee guida UNI CEI EN ISO/IEC 27017 e UNI CEI EN ISO/IEC 27018. Erogazione del servizio di conservazione di documenti informatici. SoA rev. 00 del 24/09/2024.

UNI EN ISO 9001:2015 e UNI EN ISO 14001:2015: Erogazione di servizi di progettazione e sviluppo software e di servizi di Cloud Computing, in modalità SaaS. Erogazione del servizio di conservazione di documenti informatici.

Assistenza tecnica e supporto alla Pubblica amministrazione per i servizi in Cloud (IaaS – PaaS – SaaS).

Tutti i requisiti delle Norme di riferimento sono applicati nell'ambito del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) a esclusione dei punti indicati nella Sezione 1 Punto 3 del Manuale della Qualità e della Sicurezza delle Informazioni.

2. RIFERIMENTI E DEFINIZIONI

La normativa di riferimento applicata da SPE.IT è indicata nel "Manuale della Conservazione" al punto 3.1 e nel modulo Mod-4204 "Elenco dei documenti di origine esterna", in particolare per l'implementazione del SGSI sono state considerate le seguenti norme:

- UNI ISO 31000: 2018
- UNI EN ISO 9001:2015
- 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)

DEFINIZIONI

Asset: qualunque bene o informazione importante per il business dell'Organizzazione.

Credenziali: informazioni e strumenti utilizzati per richiedere il diritto di accedere ad una risorsa informatica. Esempi: user-id/password, certificati digitali, smartcard, ecc..

Disponibilità: Proprietà dell'informazione di essere accessibile e utilizzabile quando necessaria.

Integrità: Proprietà dell'informazione di essere completa e esatta.

Riservatezza: Proprietà dell'informazione di essere nota solo a chi ne ha il diritto.

Vulnerabilità: Debolezza di un asset o gruppo di asset che può essere sfruttata da un attaccante.

Per i termini e le definizioni utilizzati si rimanda anche alle definizioni contenute nel paragrafo 3 "Termini e Definizioni" del MSGI e a quelli contenuti nella norma ISO/IEC 27001.

3. POLITICA DELLA SICUREZZA DELLE INFORMAZIONI

La Politica per la Sicurezza delle Informazioni è riportata nel presente documento che è dettagliato anche in altre Politiche per aspetti più specifici.

SPE.IT avvalendosi di personale qualificato, mette a disposizione della propria clientela, servizi di altissimo valore per la conservazione digitale e la gestione dei processi collegati per le attività di conservazione delle seguenti tipologie di documenti:

- Fatture elettroniche;
- Immagini DICOM (Digital Imaging and Communications in Medicine);
- Documenti a fini tributari (es. Libro giornale, Libro inventari, Registro Cronologico etc.);
- Documenti clinici (referti).

Tutti i servizi erogati da SPE.IT sono conformi ai requisiti esplicitati dal Cliente e ai requisiti di leggi e regolamenti applicabili alle procedure di conservazione sostitutiva digitale.

SPE.IT crede nella leva della Qualità e della Sicurezza delle informazioni per continuare ad affermarsi e crescere nel settore della digitalizzazione dei documenti; per questo ha deciso di implementare e gestire un Sistema di gestione Integrato conforme alle norme ISO 9001:2015 e UNI CEI EN ISO/IEC 27001:2024 e normative collegate.

La Politica di Sicurezza delle Informazioni definita dalla Direzione di SPE.IT rappresenta il supporto base della sicurezza delle informazioni, la sua conoscenza e applicazione è obbligatoria per tutti i collaboratori interni ed esterni e viene opportunamente contrattualizzata con i terzi che accedono a qualunque titolo alle informazioni trattate.

SPE.IT considera prerequisito base della Politica di Sicurezza delle Informazioni la corretta definizione di un'adeguata analisi dei Rischi e delle Opportunità volta a comprendere le vulnerabilità, le possibili minacce e le conseguenti contromisure da applicare per tutelare adeguatamente gli asset e le informazioni.

La consapevolezza che in ambito informatico non sia possibile avere la certezza di aver raggiunto una condizione di totale sicurezza implica che, solo una corretta analisi dei Rischi e delle Opportunità, possa consentire la riduzione del rischio ad un livello accettabile e di mantenerlo tale con la continua e corretta applicazione del Sistema di gestione della sicurezza delle informazioni.

Gli obiettivi del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) di SPE.IT sono quelli di:

- garantire che i servizi di conservazione digitale siano attuati in conformità alle normative cogenti applicabili, investendo nel Sistema informativo e nelle infrastrutture aziendali, nella continua formazione dei collaboratori coinvolti nell'erogazione dei servizi, nell'implementazione del SGSI, e nelle attività necessarie per il raggiungimento della qualifica di conservatore accreditato Agid;
- assicurare la disponibilità dei servizi informatici, proteggendo le risorse del Sistema Informativo dalle minacce, interne o esterne, accidentali o intenzionali sia di tipo organizzativo che tecnologico;
- rispondere ai requisiti cogenti di norme e leggi applicabili all'Organizzazione per il rispetto delle quali si impegna formalmente la Direzione aziendale;
- assicurare l'adozione di procedure di gestione della progettazione, dell'applicazione e del monitoraggio del mantenimento di adeguati livelli di sicurezza delle informazioni per garantirne:
  - la Riservatezza: preservando le informazioni da accessi impropri (le informazioni devono essere accessibili solo a coloro che sono autorizzati ad accedervi);
  - l'Integrità: assicurando che ogni informazione sia realmente quella originariamente inserita nel sistema informativo e sia stata modificata in modo legittimo da soggetti autorizzati, salvaguardando l'accuratezza e la completezza delle informazioni e dei metodi di elaborazione;
  - la Disponibilità: garantendo la reperibilità dell'informazione in relazione alle esigenze di continuità di erogazione del servizio e di rispetto delle norme che ne impongono la conservazione sicura, assicurando che gli utenti autorizzati abbiano accesso alle informazioni quando necessario;
  - l'Autenticità: garantendo che l'informazione ricevuta corrisponda a quella generata dal soggetto o entità che l'ha trasmessa;
- garantire ai collaboratori interni ed esterni una corretta conoscenza delle problematiche connesse con la gestione della sicurezza delle informazioni e al trattamento dei dati, volta a migliorarne la consapevolezza in merito alle proprie responsabilità e alle Politiche aziendali connesse con il trattamento dei dati;
- formare il personale sui principi fondamentali della sicurezza delle informazioni, garantendo che le procedure operative attuate siano diffuse fra le parti interessate;
- coinvolgere i terzi interessati dalle attività dell'Organizzazione per renderli consapevoli del proprio ruolo nella gestione della sicurezza delle informazioni e dell'applicazione dei principi della Politica di Sicurezza delle Informazioni;

- controllare la corretta applicazione delle tecnologie utilizzate, e, ove possibile, perseguire il miglioramento delle stesse o la scelta di tecnologie più avanzate dal punto di vista della sicurezza delle informazioni, avendo cura di monitorare l'eventuale obsolescenza delle informazioni e del sistema informativo utilizzato per il trattamento delle stesse;
- attuare gli audit periodici necessari per identificare e prevenire eventuali situazioni di Non Conformità e attivare le opportune Azioni Correttive o l'aggiornamento dell'Analisi dei Rischi e delle Opportunità;
- selezionare e qualificare i fornitori che dovranno operare nel rispetto dei principi definiti dalla Politica di Sicurezza delle Informazioni;
- monitorare la soddisfazione del Cliente e attuare Azioni di miglioramento per la corretta applicazione del SGSI;
- gestire i dati in conformità a quanto previsto dal Regolamento UE 679/2016 e dal D.Lgs. 196/2003 e s.m.i. in materia di privacy, definendo le regole per la protezione dei dati fin dalla fase di progettazione dei servizi erogati (data protection by design e by default).

SPE.IT condivide la Politica di Sicurezza delle Informazioni con i propri fornitori coinvolti nelle attività del SGSI che a loro volta la condividono con tutti i potenziali interessati.

In particolare, sono tenuti a condividere e rispettare la Politica di Sicurezza delle Informazioni i fornitori di servizi informatici che, per la loro capacità di operare direttamente sui sistemi di gestione delle informazioni, possono avere un impatto rilevante sull'operatività di SPE.IT.

A tal proposito, nei contratti con tutti fornitori di servizi ritenuti critici per le attività del SGSI vengono inserite apposite clausole di riservatezza e di sicurezza delle informazioni.

4. MISSION E VISION

La Direzione di SPE.IT ha individuato nell'applicazione del Sistema di Gestione Qualità, Ambiente e Sicurezza delle Informazioni la leva strategica con la quale affrontare le continue sfide del mercato e, garantire la conformità dei servizi offerti al Cliente per la conservazione digitale, attuata nel pieno rispetto della normativa cogente applicabile.

SPE.IT vuole essere per i propri Clienti il partner di riferimento per la conservazione digitale dei documenti necessari per la gestione delle diverse attività aziendali.

Pertanto, la mission di SPE.IT è garantire il corretto trattamento dei dati conservati assicurando la riservatezza, l'integrità, autenticità e la disponibilità delle informazioni, che sono mantenute protette da accessi non autorizzati e manipolazioni che le potrebbero alterare.

SPE.IT eroga i propri servizi avvalendosi di personale qualificato che utilizza importanti risorse tecniche, offrendo ai propri Clienti servizi e consulenza per migliorare i processi di conservazione sostitutiva digitale.

SPE.IT vuole affiancare i propri Clienti per implementare e migliorare la digitalizzazione delle informazioni aziendali, attuata per garantire la corretta transizione verso la gestione dei processi digitali, necessari per consentire lo sviluppo dinamico e sicuro delle diverse attività operative.

La vision di SPE.IT è quella di garantire nel tempo ai Clienti un veloce e sicuro accesso alle informazioni necessarie per la gestione e lo sviluppo delle diverse attività aziendali.

5. COINVOLGIMENTO E RESPONSABILITÀ DELLE RISORSE UMANE

La Direzione di SPE.IT si impegna affinché il SGSI venga accettato, compreso e condiviso da parte di tutto il personale e ritiene che il pieno coinvolgimento dello stesso nell'applicazione del Sistema sia necessario affinché ogni collaboratore possa trattare e conservare correttamente le informazioni e possa prendere atto ed applicare i meccanismi di sicurezza e protezione dei dati conservati.

Le risorse umane di SPE.IT sono così organizzate:

- risorse dell'area Tecnico - Commerciale che sono responsabili dell'erogazione dei servizi legati alle telecomunicazioni (TEC): attività impiantistica IMP e attività sistemistica SIS;
- risorse dell'area Cyber Security che sono responsabili della sicurezza informatica dell'Organizzazione (RCS);
- risorse dell'area Progettazione e sviluppo software che si occupano della progettazione e della realizzazione dei prodotti software (sia quelli destinati al Cliente, sia quelli ad uso interno): area progettazione e sviluppo software, area progettazione e sviluppo software intelligenza artificiale ed image processing, assistenza clienti; PRG, PRGIAP, AC);
- risorse dell'area acquisti ACQ;
- risorse dell'area amministrativa AMM;
- funzione Compliance NMT;
- responsabile del servizio di Prevenzione e Protezione RSPP;
- responsabile del Sistema di Gestione Integrato RSI;
- responsabile Protezione dei Dati DPO;

Erogazione del servizio di conservazione di documenti informatici

- responsabile del servizio di Conservazione RSC;
- responsabile della Sicurezza dei Sistemi per la Conservazione SSC;
- responsabile della Funzione Archivistica di Conservazione RFA;
- responsabile del Trattamento dei Dati RTA;
- responsabile dei Sistemi Informativi per la Conservazione SIC;
- responsabile Sviluppo della Manutenzione del Sistema di Conservazione SMC.

I ruoli, le responsabilità e le autorità formalizzate in questo documento ed in allegato sono rivisti almeno una volta l'anno, nell'ambito del riesame del sistema, o secondo necessità.

6. PRIVACY

SPE.IT rispetta la normativa nazionale ed Europea in materia di privacy per quanto riguarda la protezione dei dati.

La struttura organizzativa di SPE.IT per la corretta applicazione del Regolamento UE 679/2016 è strutturata come di seguito indicato:

- **Titolare del trattamento:** esercita il potere decisionale sulle finalità e sulle modalità del trattamento dei dati ivi compreso il profilo della sicurezza; questi è responsabile delle scelte in materia di sicurezza dei dati trattati e in caso di mancata adozione di adeguate misure di sicurezza ne risponde anche penalmente;
- **Responsabili del trattamento:** sono scelti fra le figure aziendali che forniscono idonea garanzia del pieno rispetto delle disposizioni in materia di protezione dei dati personali, ivi compreso il profilo della sicurezza; i responsabili agiscono in base alle istruzioni specifiche ricevute dal titolare e rispondono della loro ingiustificata inosservanza, e hanno obblighi specifici circa la comunicazione di eventuali problematiche la cui risoluzione comporta l'intervento decisionale del Titolare;
- **Amministratori di Sistema:** sono figure essenziali per la sicurezza delle banche dati e la corretta gestione delle reti telematiche. Sono esperti chiamati a svolgere le funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali, ad essi è affidato spesso anche il compito di vigilare sulla protezione dei sistemi informativi;
- **Incaricati/Addetti al trattamento dei dati:** soggetti che, nominati direttamente dal Titolare del trattamento, operano sotto la sua diretta autorità nel rispetto delle istruzioni ricevute e condivise.

SPE.IT fornisce ai propri dipendenti, collaboratori, fornitori o consulenti, istruzioni organizzative e tecniche che consentono l'osservanza degli obblighi di legge relativi alla privacy, delineando il quadro delle misure di sicurezza adottate per il sistema informativo, e definendo tutte le misure per garantire l'affidabilità delle componenti hardware e software ai fini della tutela dei dati personali trattati.

SPE.IT, predisponendo specifiche informative, provvede a comunicare agli utenti dei servizi le misure di sicurezza messe in atto per proteggere e conservare i dati personali.

7. ACCESSO A BANCHE DATI DI S.P.E.

SPE.IT considera i sistemi di elaborazione delle informazioni come strumenti di lavoro ed il loro utilizzo, da parte di coloro che vi operano a qualsiasi titolo è regolamentato secondo quanto previsto dalla documentazione del SGSI.

Le banche dati, cui sono autorizzati ad accedere il personale ed i collaboratori di SPE.IT sono quelle segnalate nel registro dei Trattamenti previsto dal Regolamento UE 679/2016. Le attività di trattamento dati (sia informatici che cartacei) devono essere sempre strettamente pertinenti alle mansioni svolte e alle finalità previste nel rispetto dei principi fondamentali sanciti dall'art. 5 del Regolamento UE 679/2016.

Per la corretta gestione dei dati trattati il personale ed i collaboratori di SPE.IT si devono attenere alle indicazioni riportate nelle "Regole di comportamento" definite dalla Direzione aziendale e condivise con tutto il personale.

SPE.IT perseguirà a norma di legge i collaboratori interni ed esterni che utilizzeranno in modo non appropriato il Sistema Informativo aziendale compromettendo la sicurezza delle informazioni trattate.