Politica Integrata

Rev	Del	Descrizione	Approvazione
0	25/02/2019	Prima emissione	*OK*
1	09/09/2019	Indicazione responsabilità in ambito di sicurezza	*OK*
2	15/07/2020	Transizione norma ISO 20000:2018	*OK*
3	16/11/2021	Indicazione specifica indirizzamento alle norme	*OK*
4	03/02/2022	Inseriti riferimenti politica ISO 37001	*OK*
5	23/03/2023	Inseriti riferimenti per segnalazione cartacea per funzione anticorruzione	*OK*
6	02/05/2024	Inserimento riferimenti a qualificazione marketplace ACN per i servizi SaaS	*OK*
7	14/04/2025	Inseriti riferimenti nuova versione norma ISO/IEC 27001:2022. Modificato riferimento indirizzo sede operativa	*OK*
8	26/01/2026	Inseriti riferimenti alla NIS2	*OK*

Livello di classificazione: **Interno**

Si.net Servizi Informatici S.r.l. è una società costituita nel 2002 che si occupa di erogare servizi informatici ad enti pubblici ed aziende.

La qualità della gestione dell'organizzazione interna e dei servizi erogati è da sempre stato un obiettivo fondamentale dell'azienda, che ne tempo ha deciso di affiancare alla certificazione di Qualità ISO 9001 anche la certificazione ISO 20000 ottenuta la prima volta nell'anno 2010 e, successivamente anche la certificazione ISO 27001. Ora è intenzione di Si.net ottenere anche la certificazione ISO37001.
SI.net ha pertanto deciso di adottare un Sistema di Gestione Integrato qualità, service management e sicurezza delle informazioni nel rispetto delle normative:

- UNI EN ISO 9001:2015
- UNI EN ISO 20000:2018
- ISO/IEC 27001:2022 con controlli aggiuntivi ISO 27017 e ISO 27018.
- ISO/IEC 37001:2016 (sistema in fase di preparazione)
- Qualificazione ACN per l'erogazione dei servizi SaaS per la pubblica amministrazione
- DLGS n.138 del 04/12/2024 - Direttiva UE2022/2555 (NIS2)– Linee Guida ACN

La certificazione ISO 9001 riguarda tutta l'attività aziendale.
La certificazione ISO 2000 riguarda il servizio di gestione dei sistemi informatici di enti pubblici ed aziende.
La certificazione ISO 27001 (con controlli aggiuntivi 27017 e 27018) riguarda l'erogazione di servizi cloud SaaS, IaaS e PaaS.
La qualificazione ACN al marketplace riguarda l'erogazione di servizi SaaS per la pubblica amministrazione.
Le direttive in tema NIS2 riguardano l'innalzamento delle misure di sicurezza cyber a livello europeo.

SI.net si impegna in un'attività costante di monitoraggio di strumenti e presidi volti a contrastare ogni forma di corruzione, attiva e passiva, diretta e indiretta che coinvolga il personale di SI.NET e ciascun soggetto che svolga attività per conto della stessa.
Garantisce, inoltre, il rispetto delle normative vigenti, sia nei rapporti fra privati che nei confronti della Pubblica Amministrazione.
Per rafforzare questo impegno, la Società ha allineato il proprio sistema di gestione anticorruzione alla norma UNI ISO 37001 – Anti Bribery management Systems, pubblicata nel 2016.
Si tratta dell'unico standard riconosciuto a livello internazionale che permette di implementare un sistema di gestione finalizzato alla prevenzione e alla lotta alla corruzione in ambito aziendale e che specifica le misure e i controlli adottabili da un'organizzazione per monitorare le proprie attività aziendali ed incrementare l'efficacia di prevenzione del fenomeno.

La presente Politica è parte integrante di un più ampio sistema di etica d'impresa e di controllo interno, finalizzato a garantire la compliance alle norme e agli standard nazionali e internazionali e a tutelare la reputazione dell'impresa. Essa concorre ad aumentare il grado di conformità generale alle leggi, ai regolamenti e alle buone pratiche internazionali applicabili e, al fine di dare concreta attuazione ad una cultura aziendale ispirata al valore dell'onestà, ai comportamenti eticamente corretti, alla prevenzione e al contrasto della corruzione.

Ciascun soggetto che effettui attività per conto di SI.NET è tenuto a leggere e comprendere i contenuti della presente Politica e a comportarsi in conformità a quanto da essa stabilito.

Il personale di SI.NET, nello svolgimento delle proprie attività, si attiene a principi etici di trasparenza, chiarezza, correttezza, integrità ed equità.
In particolare, nei rapporti e nelle relazioni d'affari, sono proibiti comportamenti e pratiche che possano anche solo apparire illegali o collusivi, pagamenti che possano apparire illeciti, tentativi di corruzione e favoritismi, sollecitazioni, dirette o indirette, di vantaggi personali e di carriera per sé o per altri e più in generale atti contrari alle leggi e ai regolamenti applicabili.
L'organo direttivo di SI.NET (individuato nel Consiglio di Amministrazione della Società) si impegna a garantire un adeguato sistema di controllo interno e a guidare tutta l'organizzazione nel

raggiungimento di performance previste per la prevenzione della corruzione in coerenza con le seguenti linee guida:

- garantire un impegno continuo a condurre le proprie attività nel pieno rispetto degli obblighi normativi, verificando costantemente la corretta ed adeguata applicazione delle norme in materia di contrasto alla corruzione e dei requisiti del Sistema di gestione Anti-Corruzione;
- vietare ogni forma di corruzione e anzi incoraggiare i dipendenti alla segnalazione di sospetti in buona fede senza timore di ritorsioni e considerare la trasparenza e la legalità un valore aggiunto, integrando nei propri processi i controlli e le azioni di miglioramento necessarie a gestire la prevenzione della corruzione;
- adire le opportune azioni disciplinari o legali nei confronti dei soggetti che abbiano tenuto un comportamento illegittimo in contrasto con i principi della presente politica.

Tali indirizzi sono tradotti in obiettivi operativi definiti in uno specifico documento, costantemente monitorati in sede di Riesame dell'Alta Direzione (individuata nel Direttore Generale) e comunicati a tutta l'organizzazione nei mezzi e canali opportuni.
SI.NET si impegna a migliorare continuamente il proprio Sistema di Gestione per la Prevenzione della Corruzione e garantisce l'autorità (definita attraverso le responsabilità attribuite alla funzione e rese note a tutto il personale aziendale) e l'indipendenza (garantita dal non coinvolgimento nelle attività individuate a rischio corruzione) della Funzione di Conformità per la prevenzione della corruzione, nominata dall'Alta Direzione.

Chi opera in nome e per conto di SI.NET è consapevole di incorrere, in caso di comportamenti di tipo corruttivo e di violazione delle Legge in materia di corruzione, in illeciti sanzionabili non solo sul piano penale e amministrativo, ma anche sul piano disciplinare aziendale.

SI.NET richiede ai propri "Soci in affari" il rispetto delle Leggi vigenti, del codice etico e della presente Politica, sulla base di clausole la cui inosservanza implica la risoluzione del contratto.

SI.NET, ritenendo lo strumento della segnalazione efficace per contrastare il fenomeno corruttivo, incoraggia le segnalazioni, anche in forma anonima, di presunti fenomeni di corruzione attraverso una procedura di "whistleblowing" che disciplina la gestione e la verifica delle segnalazioni, a

garanzia della riservatezza del contenuto delle segnalazioni, dell'identità del segnalante e del segnalato e a tutela del segnalante da eventuali discriminazioni o ritorsioni.

In primo luogo, le segnalazioni in oggetto possono essere effettuate al seguente indirizzo di posta elettronica: segnalazionianticorruzione@sinetinformatica.it, e in secondo luogo, a mezzo di posta cartacea: SI.net servizi informatici S.r.l.- alla c.a. della Funzione Anticorruzione - Via Filippo Turati 111 – 20023 Cerro Maggiore (MI).

L'Alta Direzione dà alla presente Politica la massima diffusione, assicurandosi che sia compresa e attuata da tutto il personale dipendente; a tale scopo essa è resa disponibile sul sito internet aziendale.

La politica integrata viene definita ed aggiornata periodicamente (almeno una volta ogni 12 mesi) in stretta correlazione con le risultanze delle attività di analisi del contesto in cui l'azienda opera.

Tutti gli elementi di seguito riportati sono indirizzati alle norme:

- UNI EN ISO 9001:2015
- UNI EN ISO 20000:2018
- ISO/IEC 27001:2022 con controlli aggiuntivi ISO 27017 e ISO 27018
- ISO/IEC 37001:2016

alcuni di questi sono specifici e relativi ad una singola norma mentre altri sono relativi a più di una o tutte le norme in quanto il sistema è integrato.

In tema NIS2 si intende attuare un percorso completo di valutazione, progettazione e implementazione di misure di cybersicurezza, secondo gli standard nazionali, con il corretto presidio documentale e in piena conformità con gli obblighi previsti dal Manuale Operativo del Programma di Resilienza Cyber Nazionale.

L'attenzione al cliente ed ai portatori di interesse, la chiarezza delle modalità di erogazione dei servizi e rispondenza dei servizi erogati con quanto stabilito contrattualmente sono gli elementi di base su cui vengono strutturati i processi aziendali.

Il miglioramento continuo rappresenta inoltre un percorso che è sempre stato fondamentale per SI.net e che diventa ancora più evidente e rappresentativo dell'impostazione delle modalità di lavoro ed organizzative, oltre che degli obiettivi aziendali.

Ormai da diversi mesi si sta concretizzando un contesto operativo e di mercato molto flessibile e dinamico. Le modifiche relative ai prodotti/servizi erogati che un tempo derivavano dai mutamenti tecnologici, in questi ultimi periodi sono la conseguenza anche di cambiamenti normativi ed organizzativi.

Le norme che impattano sui servizi erogati da SI.net non sono costituite solo da quelle che diventano requisiti cogenti per l'azienda, ma diventano anche quelle che modificano l'attività e l'organizzazione dei clienti (in particolare per gli enti pubblici) e pertanto creano nuovi mercati e la possibilità di creazione di nuovi servizi che vengono strutturati e gestiti secondo il sistema di qualità già ampliamente collaudato.

La direzione aziendale ed il top management si impegnano ed assumono un ruolo attivo sia nella definizione della politica di qualità e del relativo sistema di gestione, sia nell'attuazione di quanto necessario per tradurre ed integrare i principi definiti all'interno dell'attività operativa dell'azienda. Gli stessi inoltre assicurano che la politica sia comunicata, compresa, attuata ed implementata da tutti i dipendenti e collaboratori, oltre che condivisa con gli stakeholder.

Oltre a quanto sopra indicato si elencano ulteriori elementi che sono il fondamento dell'orientamento alla qualità dell'attività aziendale e delle decisioni del management, impegnandosi altresì a:

- Aderire e conformarsi a tutti i requisiti delle normative volontarie sopraindicate;
- Rispettare tutti i requisiti di legge, i regolamenti, le direttive (locali, nazionali e comunitarie) applicabili alla realtà dell'Organizzazione, nel rispetto di tutte le parti interessate e delle esigenze dalle stesse espresse durante l'erogazione del servizio;
- Garantire l'efficacia e l'efficienza dei processi aziendali;

- Porre la massima attenzione nell'individuazione e nella soddisfazione delle esigenze e aspettative dei clienti, siano essi esterni o interni (uffici), ed a migliorare nel tempo il grado di soddisfazione dei clienti;
- Controllare l'operato di fornitori in outsourcing che effettuano attività che possono impattare sulla qualità dei servizi e delle forniture erogate da Si.net assumendosi la responsabilità dei processi in outsourcing
- Rendere disponibile il presente documento a tutte le parti interessate, attivare adeguati canali di comunicazione al proprio interno e verso l'esterno;
- Monitorare e migliorare costantemente il proprio Sistema di Gestione Qualità e del Service Management, definendo obiettivi per il miglioramento e verificandone, in sede di Riesame della Direzione, il raggiungimento, dandone opportuna comunicazione a tutto il personale;
- Sviluppare programmi, obiettivi, traguardi e, per il loro espletamento, mettere a disposizione risorse umane preparate, efficienti ed in misura sufficiente, nonché risorse materiali adeguate;
- Considerare i clienti come elemento fondamentale del proprio successo, lavorando per la loro soddisfazione anche riguardo alle regole di Responsabilità Sociale;
- Identificare rischi, opportunità e pericoli derivanti dallo svolgimento delle attività
- Effettuare periodicamente un riesame della politica e del sistema di gestione per verificare ed assicurare la loro congruenza, adeguatezza, efficacia ed appropriatezza nei confronti dell'organizzazione, al fine di consentire la definizione degli obiettivi di miglioramento continuo;
- Effettuare periodicamente audit interni ed audit di commessa;
- Analizzare e tenere monitorate le non conformità;
- Proteggere e garantire la riservatezza delle informazioni, proteggendole da accessi non autorizzati, da divulgazioni a personale non autorizzato.
- Rispettare durante l'erogazione dei servizi le politiche di sicurezza definite sia internamente che dal cliente.
- Proteggere e salvaguardare l'integrità delle informazioni da modifiche non autorizzate;
- Garantire la disponibilità delle Informazioni: definire un sistema di backup e ridondanza atto a mantenere la continuità operativa;
- Definire e documentare procedure per la comunicazione tempestiva e la gestione di incidenti in caso di minaccia alla Sicurezza delle Informazioni o alla Gestione del Servizio;

- Diffondere la conoscenza all'interno di SI.net delle tematiche relative alla sicurezza, alla segretezza dei dati personali per aumentarne la consapevolezza;
- Disponibilità delle Informazioni: definire un sistema di backup e ridondanza atto a mantenere la continuità operativa dei servizi; Gli elementi necessari per garantire la continuità di erogazione del servizio sono prima mappati ed identificati e su questi sono definiti gli strumenti e le modalità da implementare.

Il documento Politiche di sicurezza IT per il sistema informatico aziendale dettaglia ogni aspetto relativo alle politiche di sicurezza definite e descrive le specifiche misure implementate.
Per i servizi cloud, all'interno della documentazione tecnica del servizio vengono descritte le modalità di erogazione, la gestione degli accessi, le comunicazioni ai customer in caso di change e agli interessati in caso di data breach, il ciclo di vita degli account.

Ruoli e responsabilità per la sicurezza delle informazioni e per la corretta gestione del servizio sono definite. Fanno capo alla funzione aziendale SIS le responsabilità relative alla sicurezza informatica del sistema informatico interno e le risorse necessarie per l'erogazione del servizio, fungendo anche da owner di tutti gli elementi che lo costituiscono. Fanno capo a CLD le responsabilità relative alla sicurezza informatica degli ambienti cloud, fungendo anche da owner di tutti gli elementi che lo costituiscono.

L'analisi del rischio effettuata introduce l'analisi di rischi aggiuntivi derivanti dall'erogazione dei servizi Cloud e di conseguenza dell'utilizzo di una nuova infrastruttura. I risultati emersi da queste analisi aggiuntive vengono recepite e valutate al fine di definire specifici piani di trattamento e misure finalizzati alla protezione dei dati dei clienti. L'analisi del rischio sul servizio viene effettuata sugli asset interessati all'erogazione del servizio per individuare gli elementi che necessitano di un trattamento per ridurre il rischio. Tenendo conto dei contratti esistenti con terze parti, vengono identificati i rischi derivanti da rapporti con esterni inserendoli all'interno della valutazione generale.
La metodologia e l'analisi dei rischi viene riesaminata ad intervalli di tempo definiti, per garantire la sicurezza del servizio e le opportunità di miglioramento. Applicando il processo di analisi e gestione dei rischi, è possibile avere in qualsiasi momento lo stato di sicurezza implementato sulle risorse aziendali al fine di avere percezione sul livello di rischio associato al servizio.

La direzione attraverso l'implementazione del sistema di gestione della sicurezza delle informazioni ed in particolare delle politiche di sicurezza IT fornisce il pieno supporto e commitment all'organizzazione ai fini di raggiungere la compliance de requisiti cogenti in materia di trattamento di dati personali.

La direzione ritiene cha la politica così definita sia appropriata alle finalità di SI.net Servizi Informatici S.r.l. ed al contesto in cui la stessa opera. Affinché tali principi ed impegni diventino operativi, la direzione assicura il massimo supporto unitamente al coinvolgimento ed alla fattiva collaborazione di tutto il personale.

La Direzione

_____