POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Rev. 01 del 24/03/2026

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Introduzione
NEW Srl è una azienda fondata nel 1999 con sede a Trissino (VI) che offre soluzioni business in ambito ICT e ISP (Internet Service Provider). In particolare, i servizi offerti dall'azienda sono:
-realizzazione e assistenza di infrastrutture IT
-fornitura, installazione e configurazione di dispositivi di rete e networking
-fornitura di connessioni internet e linee voce (servizi ISP)
-realizzazione, installazione e assistenza di sistemi telefonici e di unified communication & collaboration
-monitoraggio e sicurezza delle infrastrutture IT, cybersecurity
-servizi internet (gestione domini, hosting, housing, posta elettronica)
-soluzioni cloud e datacenter (backup cloud, server cloud, soluzioni SaaS e IaaS)

Scopo
Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni definiti da NEW Srl al fine di sviluppare un efficiente e sicuro Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), stabilire il quadro di riferimento per gli obiettivi da perseguire e l'impegno della Direzione al soddisfacimento dei requisiti applicabili e al miglioramento continuo delle prestazioni.

Politica per fissare gli obiettivi di sicurezza
Grazie all'implementazione del sistema di gestione, abbiamo determinato gli obiettivi di sicurezza delle informazioni che ci vedranno impegnati, in ciascun processo aziendale, alla preservazione della:

- Riservatezza: assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati e che le informazioni non siano rese disponibili o divulgate a persone o entità non autorizzate;
- Integrità: salvaguardare la consistenza dell'informazione da modifiche non autorizzate e garantire che l'informazione non subisca modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici;
- Disponibilità: assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta.

Politica per l'impegno al rispetto dei requisiti applicabili
Per le caratteristiche dei servizi che la società offre ai propri clienti e per il valore che rappresentano le informazioni nel proprio business, la politica per la sicurezza delle informazioni rappresenta un indirizzo strategico fondamentale. Per perseguire l'obiettivo primario la Direzione pone grande attenzione alla progettazione, alla gestione e alla manutenzione della propria struttura tecnologica, fisica, logica ed organizzativa. La Direzione impegna, quindi, la propria organizzazione a sviluppare e manutenere un sistema di gestione per la sicurezza delle informazioni nell'ambito delle attività svolte e dei servizi erogati in accordo ai requisiti della norma ISO/IEC 27001:2022, che rappresenta lo standard internazionale di riferimento per preservare la riservatezza, l'integrità e la disponibilità delle informazioni.
Per questo, l'alta direzione assume l'impegno di esercitare la leadership secondo quanto stabilito da tale Norma.

Politica per l'impegno per il miglioramento continuo del sistema di gestione
Il patrimonio informativo del cliente e quello relativo al know-how della nostra organizzazione costituiranno d'ora innanzi i punti focali dell'impegno di tutti. Un impegno assunto da tutti e da ciascuno.

Tale impegno sarà manifestato attraverso le "performance di sicurezza" che dovranno dare evidenza di quanto la nostra organizzazione ed il nostro sistema di gestione della sicurezza delle informazioni siano efficaci nel registrare un miglioramento continuo.

Politica per la sicurezza delle informazioni

La nostra azienda offre servizi informatici e di telecomunicazione ai propri clienti, appartenenti a tutti i settori di mercato, pubblico e privato. Trattiamo quindi dati pubblici e riservati, dati personali comuni o sensibili, dati anche ad alta criticità.

Data la potenziale criticità dei dati trattati, in qualunque formato essi siano (informatico e non), è fondamentale che sia loro garantita la massima sicurezza. Questo si traduce nella salvaguardia della loro riservatezza in particolare e anche della loro integrità e disponibilità.

I livelli di sicurezza da garantire devono essere tali da rispettare le clausole contrattuali e la normativa vigente, nonché da garantire la coerenza e il bilanciamento tra: rischio di impresa, sostenibilità economica, risultati delle analisi e valutazione del rischio, politiche e strategie aziendali, politiche e strategie dei fornitori e dei clienti, necessità di costante adeguamento al contesto in cui operiamo e di miglioramento dell'efficacia ed efficienza dei nostri processi e controlli di sicurezza.

I principi cardine a cui attenersi sono:

- le informazioni devono essere accessibili solo a coloro che ne hanno necessità (principio *need to know*) e nei tempi stabiliti;
- i dati e le informazioni devono essere protetti, tramite la messa in opera di idonee contromisure logiche, fisiche e organizzative, da accessi non autorizzati;
- l'organizzazione deve mantenere aggiornata e monitorata la propria infrastruttura tecnologica per prevenire attacchi informatici o fuga di informazioni
- i dati e le informazioni contenute nei sistemi informativi devono essere prontamente a disposizione degli utenti autorizzati nel momento in cui le richiedono;
- i dati personali, che l'organizzazione custodisce a qualsiasi titolo (Titolare del trattamento o Responsabile del trattamento nominato da Titolari esterni) devono essere trattati nel pieno rispetto degli obblighi di legge (Regolamento UE 2016/679 sulla protezione dei dati personali; normative e provvedimenti nazionali in materia di protezione dei dati personali);
- l'organizzazione deve operare nel pieno rispetto della legge sui diritti di proprietà intellettuale nell'utilizzo di pacchetti software commerciali e di altro materiale coperto dal diritto d'autore;
- il personale deve essere opportunamente formato in materia di sicurezza delle informazioni e deve seguire i principi etici e comportamentali prescritti;
- i fornitori devono essere opportunamente tenuti sotto controllo attraverso misure da stabilire a seconda dei casi;
- i partner devono essere selezionati anche per la loro capacità e disponibilità a conformarsi alle nostre regole di sicurezza;
- per i servizi erogati, è necessario considerare i requisiti di sicurezza sin dalla contrattazione con il cliente.

NEW Srl, nell'erogazione di servizi cloud (backup cloud, server cloud, housing, hosting, colocation), opera in qualità di Cloud Service Provider (CSP) e di Responsabile del Trattamento ai sensi dell'art. 28 del Regolamento UE 2016/679 (GDPR). In tale ruolo, le informazioni di identificazione personale (PII) trattate per conto dei clienti (Cloud Service Customer — CSC) sono soggette ai controlli specifici previsti dalle norme ISO/IEC 27017:2015 per la sicurezza dei servizi cloud e ISO/IEC 27018:2025 per la protezione delle PII nel cloud. Le PII sono trattate esclusivamente su istruzione documentata del CSC, con garanzie di riservatezza, segregazione, cancellazione sicura e notifica tempestiva in caso di violazione.

Impegni della Direzione

La politica della sicurezza rappresenta in concreto l'impegno della Direzione nei confronti di clienti e delle terze parti a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività.

La Direzione con la presente politica si impegna a garantire che:

- l'organizzazione abbia piena conoscenza delle informazioni gestite e valuti di volta in volta la loro criticità, al fine di agevolare l'implementazione di adeguati livelli di protezione;
- l'accesso alle informazioni avvenga in modo sicuro e adatto a prevenire i trattamenti non autorizzati o realizzati senza i diritti necessari;
- l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza;
- l'organizzazione e le terze parti, che collaborano al trattamento delle informazioni, siano adeguatamente formate e abbiano piena consapevolezza delle problematiche relative alla sicurezza;
- le anomalie e gli incidenti aventi ripercussioni sul sistema informativo, sui servizi e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business;
- l'accesso alla sede ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti;
- siano assicurati la conformità ai requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti;
- la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi siano gestiti al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni;
- la business continuity aziendale siano attuati attraverso l'applicazione di procedure di sicurezza stabilite;
- i trattamenti dei dati personali, sia nei casi in cui la società operi in qualità di Titolare che nei casi in cui operi per conto terzi in qualità di Responsabile del Trattamento, avvengano nel rispetto del Regolamento Europeo sulla Protezione dei Dati Personali GDPR 679/2016;
- nel ruolo di Cloud Service Provider, la conformità ai requisiti della norma ISO/IEC 27017:2015 per la sicurezza dei servizi cloud e della norma ISO/IEC 27018:2025 per la protezione delle PII nel cloud, assicurando che i clienti CSC siano informati sui luoghi di trattamento, sui sub-processor coinvolti e sulle modalità di gestione degli incidenti che li riguardano.

La Direzione si impegna infine a:

- adottare un sistema di gestione sicura delle informazioni conforme ai requisiti specificati della norma ISO/IEC 27001 e, per i servizi cloud, delle norme ISO/IEC 27017:2015 e ISO/IEC 27018:2025;
- mantenere costantemente monitorato il grado di conformità del sistema alle norme e leggi applicabili di natura cogente e volontaria, e gli obblighi contrattuali pertinenti l'ambito di applicazione del SGSI;
- garantire mezzi e risorse idonee al suo mantenimento e miglioramento continuo, in particolare per quanto attiene la mitigazione/riduzione dei livelli di rischio sulla sicurezza delle informazioni e l'adozione di misure idonee a prevenire situazioni anomale e di emergenza;
- rendere consapevoli tutte le persone che dell'organizzazione degli obblighi e delle responsabilità di ciascuno nella gestione della sicurezza delle informazioni e delle conseguenze in caso di eventi, dolosi e colposi, relativi all'utilizzazione non autorizzata, modifica o distruzione di informazioni critiche.

La politica della sicurezza delle informazioni viene costantemente aggiornata e verificata, attraverso un riesame annuale, per assicurare la coerenza con le finalità strategiche dell'organizzazione. La politica è condivisa con l'organizzazione, le terze parti ed i clienti, attraverso la sua pubblicazione sul sito web.

Data: 24/03/2026

NEW SRL

NEW SRL
Viale Dell'Industria, 93 int. 12 - 36070 TRISSINO (VI)
Tel. 0445-446749 - Fax 0445-459434
Cod. Fisc. E Part. IVA 02782600247