POLITICA PER LA SICUREZZA DELLE INFORMAZIONI
RIFERIMENTO NORMA: ISO/IEC 27001

Nome del documento		PIANO DELLA QUALITA'	
Emesso da		DotEnv S.r.l.	
Redatto da		Simone Checcoli (RSGI)	
Approvato da		Direzione	
Versione	00	Pagine	
Data di Prima Emissione		25/06/2025	
Classificazione		Pubblico	

RIEPILOGO REVISIONI E VERSIONI PRECEDENTI

Versione	Data emissione	Sintesi modifiche	Eseguite da
00	25/06/2025	Rilascio	Simone Checcoli

1. PREMESSA GENERALE

Dotenv s.r.l. è una società che fornisce servizi specializzati di gestione, manutenzione e monitoraggio di infrastrutture e sistemi informatici per conto di terzi. L'attività principale consiste nell'assicurare la continuità operativa, la disponibilità e la sicurezza dei dati e delle applicazioni ospitate sulle infrastrutture IT dei propri clienti.

2. IMPEGNO DELLA DIREZIONE E OBIETTIVI

L'obiettivo primario che l'Azienda si pone è la protezione dei dati e delle informazioni al fine di tutelare i dati dei Clienti e delle persone fisiche di cui si trattano i dati personali. Per le caratteristiche dei servizi che Dotenv 4.0 S.r.l. offre ai propri clienti e per il valore che rappresentano le informazioni nel proprio business, la Politica della Sicurezza delle Informazioni rappresenta un indirizzo strategico fondamentale e prioritario. Il Sistema di Gestione per la Sicurezza delle Informazioni è fondato sul rispetto di:

- riservatezza: assicurare che l'informazione sia accessibile solamente ai soggetti debitamente autorizzati nell'ambito dei processi gestiti;
- integrità: salvaguardare contenuti e consistenza dell'informazione da modifiche non autorizzate;
- disponibilità: assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati, quando ne fanno richiesta;
- controllo: assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
- privacy: garantire la protezione e il controllo dei dati personali e del loro trattamento.

Tutte le persone che lavorano e/o collaborano con Dotenv 4.0 s.r.l. (compresi Fornitori, Clienti e Partner) sono impegnate a rispettare questi principi.

Dotenv 4.0 s.r.l. ha definito attraverso il SGSI i seguenti obiettivi:

- avere una visione complessiva e centrale della sicurezza aziendale, che spazia oltre il perimetro della sicurezza IT includendo anche persone e processi;
- dimostrare la sua abilità nel fornire prodotti e servizi conformi ai requisiti dei clienti, ai requisiti degli standard di riferimento, delle leggi e dei regolamenti applicabili;
- incrementare la soddisfazione dei clienti attraverso l'efficace applicazione del SGSI e dei processi di miglioramento continuo e assicurando il rispetto dei requisiti stabiliti dalle normative cogenti e dai regolamenti applicabili.

3. IL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

Dotenv 4.0 s.r.l. si impegna da sempre ad applicare i principi della Privacy by Design e Privacy by Default nella progettazione, gestione e manutenzione della propria struttura tecnologica, fisica, logica e organizzativa. Dotenv 4.0 s.r.l. ritiene che la sicurezza delle informazioni rappresenti un fattore dirimente di successo sia per quanto riguarda i processi di progettazione e sviluppo di soluzioni tecnologiche che per quanto riguarda l'erogazione dei servizi. La politica per la sicurezza delle informazioni è costituita da un insieme di attività che comprendono: l'identificazione delle aree critiche; la gestione dei rischi, dei sistemi e della rete, delle vulnerabilità e degli incidenti; il controllo degli accessi; la gestione della privacy e della compliance; la valutazione dei danni e tutti gli altri aspetti che possono impattare sulla gestione della sicurezza delle informazioni.

L'organo direttivo è fortemente impegnato ad una grande responsabilizzazione di tutte le persone che lavorano per e con la società nel garantire la rigorosità del proprio operato per adempiere, con la massima attenzione, ai compiti assegnati.
In particolare, questo obiettivo è perseguito attraverso l'impegno a garantire:
1. il rispetto delle leggi e normative vigenti;
2. l'efficienza operativa e affidabilità dei processi di sviluppo di prodotti e servizi correlati;
3. le condizioni di salute e sicurezza sui luoghi di lavoro per il personale e terzi;
4. la continuità e l'efficienza dei processi organizzativi e operativi al fine di prevenire e ridurre al minimo l'impatto degli incidenti volontari o casuali sulla sicurezza dei dati/informazioni gestite;
5. la protezione degli strumenti resi disponibili e il loro corretto utilizzo;
6. la riservatezza, la correttezza e la disponibilità dei dati/informazioni gestiti da Dotenv 4.0 s.r.l. e la salvaguardia della proprietà intellettuale;
7. l'adozione di misure di prevenzione di anomalie di processo/prodotto/servizio.

Per dare attuazione alla propria politica della sicurezza delle informazioni, Dotenv 4.0 s.r.l. ha sviluppato e si impegna a mantenere un sistema di gestione sicura delle informazioni conforme ai requisiti specificati, delle norme UNI CEI EN ISO/IEC 27001 e delle leggi cogenti come mezzo per gestire la sicurezza delle informazioni nell'ambito della propria attività. Nell'ambito della gestione dei servizi offerti, l'organizzazione assicura:
- l'osservanza dei livelli di sicurezza stabiliti attraverso l'implementazione SGSI (sistema di gestione della sicurezza delle informazioni);
- il rispetto delle normative vigenti e degli standard internazionali di sicurezza per la propria infrastruttura tecnologica e organizzativa;
- la selezione di partner affidabili dal punto di vista della gestione in sicurezza delle informazioni e della protezione dei dati personali.

3.1. CAMPO DI APPLICAZIONE

La presente politica si applica indistintamente a tutti gli organi e i livelli dell'Azienda. L'attuazione della presente politica è obbligatoria per tutto il personale e deve essere inserita nella regolamentazione degli accordi con qualsiasi soggetto esterno che, a qualsiasi titolo, possa essere coinvolto con il trattamento di informazioni che rientrano nel campo di applicazione del Sistema di Gestione (SGSI): il campo di applicazione è:

"Progettazione, sviluppo e assistenza di soluzioni software e applicativi"

Oltre al personale interno, la politica per la sicurezza delle informazioni si applica anche alle terze parti che collaborano/intervengono nei processi e alle risorse coinvolte nella progettazione, realizzazione, avviamento ed erogazione continuativa nell'ambito dei servizi.
L'impegno è esteso all'organizzazione interna ed agli stakeholders. La PSI rappresenta in concreto l'impegno dell'organizzazione nei confronti di clienti e delle terze parti a garantire la sicurezza delle informazioni, degli strumenti fisici, logistici e organizzativi atti al trattamento delle informazioni in tutte le attività.

4. DICHIARAZIONE DI IMPEGNO

In sintesi, la politica della sicurezza delle informazioni garantisce:
a) 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;

b) che l'accesso alle informazioni avvenga in modo sicuro e adatto a prevenire i trattamenti non autorizzati o realizzati senza i diritti necessari;
c) che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza;
d) che l'organizzazione e le terze parti che collaborano al trattamento delle informazioni siano adeguatamente formate e abbiano piena consapevolezza delle problematiche relative alla sicurezza;
e) che le anomalie e gli incidenti aventi ripercussioni sul sistema informatico, 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;
f) che l'accesso alla sede ed ai singoli locali aziendali avvenga esclusivamente da parte di personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti;
g) la conformità con i requisiti di legge e il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti;
h) che vengano correttamente effettuate la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni; i) la business continuity;
l) che i trattamenti dei dati personali, sia nei casi in cui Dotenv 4.0 S.r.l. operi in qualità di Titolare che nei casi in cui operi per conto terzi in qualità di Responsabile del Trattamento, avvenga nel rispetto del Regolamento Europeo sulla Protezione dei Dati Personali GDPR 679/2016.

La politica della sicurezza delle informazioni viene costantemente aggiornata e verificata, in fase di riesame annuale del SGSI e anche qualora si manifestino condizioni contingenti che determinano nuove opportunità, per assicurare il suo continuo miglioramento. Viene quindi condivisa con l'organizzazione, le terze parti ed i clienti.

5. RESPONSABILITÀ DI OSSERVANZA E ATTUAZIONE

L'osservanza e l'attuazione delle policy sono responsabilità di:
1. tutto il personale che, a qualsiasi titolo, collabora con l'azienda ed è in qualche modo coinvolto con il trattamento di dati ed informazioni che rientrano nel campo di applicazione del Sistema di Gestione. tutto il personale è altresì responsabile della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza.
2. Tutti i soggetti esterni che intrattengono rapporti e collaborano con l'azienda, devono garantire il rispetto dei requisiti contenuti nella presente policy. Il Responsabile del Sistema di Gestione della Sicurezza delle Informazioni che, nell'ambito del Sistema di Gestione e attraverso norme e procedure appropriate, deve:

1. condurre l'analisi dei rischi con le opportune metodologie e adottare tutte le misure per la gestione del rischio
2. stabilire tutte le norme necessarie alla conduzione sicura di tutte le attività aziendali
3. verificare le violazioni alla sicurezza e adottare le contromisure necessarie e controllare l'esposizione dell'azienda alle principali minacce e rischi
4. organizzare la formazione e promuovere la consapevolezza del personale per tutto ciò che concerne la sicurezza delle informazioni.
5. verificare periodicamente l'efficacia e l'efficienza del Sistema di Gestione.

Chiunque, dipendenti, consulenti e/o collaboratori esterni dell'Azienda, in modo intenzionale o riconducibile a negligenza, disattenda le regole di sicurezza stabilite e in tal modo provochi un danno all'azienda, potrà essere perseguito nelle opportune sedi e nel pieno rispetto dei vincoli di legge e contrattuali.

6. RIESAME

L'organo Direttivo verificherà periodicamente e regolarmente o in concomitanza di cambiamenti significativi l'efficacia e l'efficienza del Sistema di Gestione, in modo da assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e in modo da favorire l'attivazione di un processo continuo, con cui viene mantenuto il controllo e l'adeguamento della policy in risposta ai cambiamenti dell'ambiente aziendale, del business, delle condizioni legali. Il riesame dovrà verificare lo stato delle azioni preventive e correttive e l'aderenza alla politica.

Dovrà tenere conto di tutti i cambiamenti che possono influenzare l'approccio della azienda alla gestione della sicurezza delle informazioni, includendo i cambiamenti organizzativi, l'ambiente tecnico, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali e dei risultati dei precedenti riesami.
Il risultato del riesame dovrà includere tutte le decisioni e le azioni relative al miglioramento dell'approccio aziendale alla gestione della sicurezza delle informazioni.

La Direzione

DotEnv S.r.l. C. Soc.: 10.000 € (i.v.)
Via Beethoven 15/C - 44124 Ferrara
P.IVA 02062960386
REA FE - 222315
T.: +39 0532 1[illegible]70 97
PEC: dotenv@pec.it
M.: info@dotenv.it
www.dotenv.it