

	Nome documento	Revisione	00
	Politica per la Sicurezza delle Informazioni Parte Generale	Data	03/02/2026
		Creato da	Responsabile Servizi Continuità
		Approvato da	Direzione
		Tipo di documento	Documento Pubblico

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Sommario

PARTE GENERALE.....	2
1. GLOSSARIO.....	2
2. OBIETTIVI	2
3. ENTRATA IN VIGORE DEL DOCUMENTO E PUBBLICITÀ	3
4. SISTEMA DI GESTIONE SICUREZZA DELLE INFORMAZIONI (SGSI)	3
5. CLASSIFICAZIONE DELLE INFORMAZIONI	5
a. Pubbliche.....	5
b. Interne	5
c. Riservate.....	5
d. Strettamente riservate (*)	5
6. GESTIONE	6
HW.....	6
SW6	
Tipologia di dati	6
Località.....	6
Requisiti per garantire la sicurezza delle informazioni	6

 	Nome documento	Revisione	00
	Politica per la Sicurezza delle Informazioni Parte Generale	Data	03/02/2026
		Creato da	Responsabile Servizi Continuità
		Approvato da	Direzione
		Tipo di documento	Documento Pubblico

PARTE GENERALE

1. GLOSSARIO

- Informazioni/e: si intendono i dati personali ai sensi del GDPR e i dati aventi, per loro natura, carattere confidenziale appartenenti alla stessa Società, ai collaboratori, ai clienti e ai fornitori della stessa.
- Gruppo: inteso come gruppo SMEUP.
- Gestione Della Sicurezza Delle Informazioni (GSI): si intende la definizione dei requisiti di sicurezza delle informazioni (interne e esterne), l'analisi dei rischi, la definizione di un piano per soddisfare quei requisiti, nonché l'implementazione del piano stesso.
- Cybersecurity: si intende l'insieme di processi, procedure e tecnologie che proteggono sistemi informatici, reti e dati da attacchi, danni o accessi non autorizzati.

INFORMAZIONI (GSI) si intende la definizione dei requisiti di sicurezza delle informazioni (interne e esterne), l'analisi dei rischi, la definizione di un piano per soddisfare quei requisiti, nonché l'implementazione del piano stesso.

2. OBIETTIVI

La progressiva diffusione delle minacce informatiche (ransomware, virus, furto delle identità, accessi non autorizzati, etc.) espone gli utenti di un sistema informatico (dipendenti e collaboratori della Società) e più in generale la Società a rischi di natura patrimoniale e a diverse forme di responsabilità conseguenti alla mancata tutela delle Informazioni e conseguente violazione di specifiche disposizioni di legge (che riguardano ad la tutela della privacy, la commissione di reati informatici..), creando evidenti problemi alla sicurezza e all'immagine della Società stessa.

Perciò, la Società ha adottato un sistema di gestione per:



- garantire la sicurezza delle Informazioni trattate sia su sistemi informatici interni che su sistemi gestiti per conto del cliente o messi a disposizione dai clienti proteggendoli da potenziali minacce;
- garantire la sicurezza dei dati e delle informazioni di proprietà della Società e/o dei clienti trattate dai fornitori;
- rispettare gli impegni contrattuali assunti con i propri collaboratori, clienti e fornitori,
- effettuare la gestione informatica dei dati in oggetto.

la Società intende, pertanto, formalizzare alcune regole di comportamento generali per gestire la sicurezza contro gli attacchi informatici ("cybersecurity") al fine di aumentare la conoscenza, la consapevolezza, le misure adottate, la formazione, la resilienza e per cercare di ridurre al minimo le minacce alla sicurezza nel trattamento delle Informazioni, al fine di evitare di esporre la Società a responsabilità di natura amministrativa o penale o comunque sanzionatoria o a rischi di natura patrimoniale.

La creazione di un sistema di gestione della sicurezza delle informazioni permette di assicurare, monitorare, mantenere, migliorare la gestione della sicurezza delle informazioni, evitare la manomissione delle stesse e la sottrazione da parte di terzi, nonché prevedere e ridurre al minimo i rischi cui i dati sono sottoposti.

I vantaggi dell'adozione di un sistema così concepito si riassumono nei seguenti punti fondamentali:

- Accrescere la consapevolezza sulla sicurezza tra lavoratori, Direzione, responsabili, clienti e fornitori,

 	Nome documento	Revisione	00
	Politica per la Sicurezza delle Informazioni Parte Generale	Data	03/02/2026
		Creato da	Responsabile Servizi Continuità
		Approvato da	Direzione
		Tipo di documento	Documento Pubblico

fornendo un sistema di procedure definite sulla base della realtà aziendale che dia risalto alla formazione ed all'informazione nonché alla responsabilità da parte di tutti gli utenti.

- Individuare i beni critici per il business dell'azienda, le Informazioni, interne o meno, fondamentali per la gestione del sistema ed il suo mantenimento.
- Garantire un sistema di regole e strutture che vada a perseguire la sicurezza delle Informazioni e delle strutture adibite alla loro conservazione.
- Fornire un sistema in cui riporre fiducia, sia all'interno che all'esterno dell'organizzazione.
- Aggiornamento e monitoraggio: arricchire cioè la conoscenza, la dimestichezza e la capacità pratica della Direzione nella gestione e nel mantenimento di un sistema di sicurezza dell'Informazione.
- Sviluppare un corretto sistema di business, attraverso riduzione del rischio di diffusione all'esterno non controllata delle Informazioni che si intendono gestire in modo sicuro.
- Continuo aggiornamento delle proprie infrastrutture tecniche ed organizzative alla luce delle esigenze riscontrate cogenti e mutevoli (compliance e contract review).
- Migliorare la gestione delle relazioni con i soggetti terzi (comunicazioni, divulgazione delle informazioni, accesso alle Informazioni aziendali, livelli di rischio).
- Compatibilità legale con le norme nazionali ed internazionali vigenti in tema di privacy e tutela dei dati personali (GDPR) e in ambito cybersicurezza (NIS 2), diritti di proprietà intellettuale, diritto d'autore, concorrenza. Nonché compatibilità con altri schemi normativi internazionali che regolano l'implementazione di altri sistemi di gestione (es. ISO 9001 Sistema di Gestione per la Qualità).
- Tutela delle credenziali di accesso ai propri sistemi informatici e alle proprie attrezzature da parte dell'utenza aziendale e dei clienti.

La Società, strutturando un sistema formato da politiche, manuali, procedure, istruzioni operative, documenti e registrazioni, persegue l'obiettivo di migliorare e mantenere il sistema, evidenziandone punti di forza e di debolezza.

Tutte le azioni che andranno a dare evidenza di un miglioramento o comunque di una gestione con particolari problematiche, saranno oggetto di registrazione e revisione annuale, per valutarne applicazione ed efficacia.

3. ENTRATA IN VIGORE DEL DOCUMENTO E PUBBLICITÀ



Molte linee guida contenute nel presente documento sono già operative nell'uso quotidiano e vengono qui formalizzate e integrate per una copertura generale e un continuo miglioramento. La data di ultimo aggiornamento è riportata in calce al documento. L'ultima versione del presente documento sostituisce tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate.

Copia della presente politica viene pubblicata nella bacheca virtuale aziendale nonché nel web site e consegnata a ciascun dipendente.

4. SISTEMA DI GESTIONE SICUREZZA DELLE INFORMAZIONI (SGSI)

La Società si prefigge quale obiettivo la protezione delle informazioni relative a:

- area commerciale
- area tecnica
- area amministrativa
- know how aziendale
- sistemi informativi dei clienti
- dati personali dei dipendenti, clienti e fornitori

 	Nome documento	Revisione	00
	Politica per la Sicurezza delle Informazioni Parte Generale	Data	03/02/2026
		Creato da	Responsabile Servizi Continuità
		Approvato da	Direzione
		Tipo di documento	Documento Pubblico

dal più ampio spettro di minacce possibile, allo scopo di assicurare la continuità delle attività della Società, minimizzare i rischi, garantire il ritorno degli investimenti, le opportunità di business, il rispetto delle leggi, la redditività dell'attività aziendale.

Tutti le Informazioni per la gestione delle attività di business della Società devono essere protette per garantire che giungano integre a chi deve utilizzarle, che non vadano disperse, che non vengano violate o che non finiscano nelle mani di concorrenti o di approfittatori in forma non autorizzata o non controllata.

L'Informazione è considerata un asset, e sono considerati altri asset le strutture materiali o immateriali che la gestiscono. Il controllo e la protezione dell'Informazione sono essenziali per l'organizzazione della Società e, pertanto, si impegna a condividere gli obiettivi ed i principi della sicurezza delle informazioni mediante la predisposizione di un sistema di operazioni e di controlli per gestire il rischio.

In particolare, con l'implementazione di questo sistema:

- Vengono analizzati i rischi.
- Vengono trattati i rischi sulla base di criteri di accettazione dei rischi stessi, in ogni caso non compromettendo il rispetto delle leggi dello Stato ed i requisiti contrattuali. Pertanto:

vengono accettati consapevolmente i rischi se soddisfano quei criteri; alternativamente:

- si evitano i rischi non permettendo azioni/attività che potrebbero essere causa dei rischi stessi;
- i rischi sono trasferiti a terze parti.

La Società rende consapevoli tutte le proprie risorse e i propri dipendenti, che operano nel vivo del sistema che gestisce le informazioni che si intendono proteggere, della necessità di operare responsabilmente mediante formazione a tutti i livelli;



La Società introduce specifiche attività di controllo e precauzione contro gli incidenti e sono disposti adeguati provvedimenti ogni qualvolta si verificheranno delle violazioni.

Il sistema messo in atto dalla Società include:

- monitoraggio di tutti gli eventi con la verifica periodica dell'efficacia dei controlli prescritti ed il successivo riesame annuale della Direzione;
- attivazione delle azioni di miglioramento;
- gestione della documentazione e delle registrazioni di sistema;
- addestramento del personale per conseguire competenza e consapevolezza sulle problematiche della sicurezza delle informazioni;
- audit interni per verificare che i controlli siano efficaci, gli obiettivi dei controlli vengono raggiunti e che le procedure vengano applicate;
- miglioramento attraverso le Azioni Correttive e Preventive.

Nell'ambito di questo sistema sono assegnate le seguenti responsabilità:

- Direzione aziendale: la definizione degli Assets da proteggere e il riesame periodico dello stato di sicurezza delle informazioni e l'efficacia della presente politica di concerto con il Security Team e Qualità.
- Security Team -: la valutazione dei rischi cui possono essere esposti i vari Assets.
- Security Team ed Amministratore di Sistema -: l'impostazione dei controlli, la loro implementazione e monitoraggio.
- Security Team ed Amministratore di Sistema: la registrazione di tutte le minacce verificatesi la pianificazione ed implementazione dei controlli necessari.
- Dipendenti che lavorano con i rispettivi assets materiali o immateriali: il rispetto delle prescrizioni e autorizzazioni redatte dalla Società e l'obbligo di segnalare al Security Team o alla Qualità eventuali minacce riscontrate.

 	Nome documento	Revisione	00
	Politica per la Sicurezza delle Informazioni Parte Generale	Data	03/02/2026
		Creato da	Responsabile Servizi Continuità
		Approvato da	Direzione
		Tipo di documento	Documento Pubblico

- Security Team e Qualità - proporre alla Direzione e intraprendere azioni di miglioramento e attivare la procedura in caso di incidente (procedura di Incident e procedura Data Breach) in caso di segnalazione.

5. CLASSIFICAZIONE DELLE INFORMAZIONI

Le informazioni trattate dalla Società per lo svolgimento della propria attività lavorativa, possono essere di diversa natura. Tali informazioni, in funzione dei possibili danni che una eventuale divulgazione potrebbe arrecare alla Società o anche ai suoi clienti, fornitori e collaboratori tutti, vengono classificate nel seguente modo, in 4 diverse tipologie:

- Pubbliche
- Interne
- Riservate
- Strettamente riservate

a. Pubbliche

Le informazioni pubbliche non richiedono alcun controllo, essendo destinate ad una fruizione pubblica.

b. Interne

Le informazioni per uso interno sono a disposizione del personale aziendale e di altri addetti che possono accedere alla rete informatica aziendale a condizione che tale accesso comporti un rischio di scarsa rilevanza.

c. Riservate



Le informazioni riservate sono rivolte a destinatari specifici e sono rigorosamente disciplinate dal principio della necessità di sapere (controlli dell'accesso). La divulgazione non autorizzata delle informazioni riservate potrebbe compromettere la reputazione della Società o comportare un pericolo per le persone.

Sono incluse in questa categoria:

- informazioni personali su singoli individui, siano essi membri del personale della Società, di terzi o di clienti;
- dati del registro di sistema;
- dati relativi a vendite e marketing;
- piani aziendali, dati di budget, dati economici, finanziari e know how della società in generale;
- dati relativi al personale;
- dati relativi ai rischi;
- password;
- informazioni riservate per obbligo di legge.

d. Strettamente riservate (*)

I dati o le informazioni strettamente riservati si caratterizzano per una diffusione circoscritta e destinata a un numero limitato di soggetti e sono rigorosamente disciplinati dal principio della necessità di sapere (è necessario sapere chi ne possiede copie e chi può accedervi). La divulgazione non autorizzata potrebbe recare un danno eccezionale alla Società. Le informazioni strettamente riservate richiedono i controlli di sicurezza più severi e pertanto l'utente è tenuto a valutarne attentamente la natura.

 	Nome documento	Revisione	00
	Politica per la Sicurezza delle Informazioni Parte Generale	Data	03/02/2026
		Creato da	Responsabile Servizi Continuità
		Approvato da	Direzione
		Tipo di documento	Documento Pubblico

6. GESTIONE

È stato definito l'elenco degli Assets che la Società si prefigge di proteggere in termini di Hw, Sw, rete, tipologia di dati, località e attività i cui dati sono immagazzinati e/o elaborati nel Sistema Informativo della società, nel Sistema Informativo dei fornitori e nei sistemi informativi dei clienti.

In particolare, gli assets protetti, inclusi quelli relativi ai requisiti legali e contrattuali, sono:

HW

Server.

Apparati di rete.

PC (Client aziendali e Notebook).

SW

Sistemi Operativi.

Software gestionali ed Applicativi.

Software di monitoraggio.

RETE.

Tipologia di dati

Documentazione, dati e registrazioni di origine interna relativa ai processi Aziendali.

Documentazione, dati e registrazioni di origine esterna (di proprietà del cliente).

Località

Datacenter Acantho Imola (BO), via Molino Rosso 8 - Imola (BO).

Datacenter Stack Infrastructure Sizzano.

Servizi di Continuità - via Molino Rosso 9/C - Imola (BO).

Le attività della Società sono fortemente dipendenti dal Sistema Informativo: l'assenza di sicurezza o anche la diminuzione del livello di sicurezza comprometterebbero la gestione di quanto sopra espresso in termini di dati.

La Società si prefigge, quindi, di perseguire i seguenti obiettivi:



- evitare l'accesso ai nostri Sistemi Informativi da parte di soggetti non autorizzati;
- evitare che le Informazioni di proprietà della Società o di proprietà dei propri clienti che vengono trasmesse ed elaborate nei Sistemi Informativi interni o nei Sistemi Informativi dei fornitori vengano modificate, rese non disponibili a chi deve utilizzarle o distrutte intenzionalmente o anche solo accidentalmente.

La Società deve anche proteggere l'Informazione che attiene alle leggi dello Stato cogenti ed al business dalla stessa perseguito.

Requisiti per garantire la sicurezza delle informazioni

I requisiti per garantire la sicurezza delle informazioni sono:

CONFIDENZIALITÀ/RISERVATEZZA: attribuzione a ciascun dipendente implicato nel sistema informativo degli accessi fisici e logici al Sistema Informativo secondo responsabilità e mansioni e verificare/accertarsi che il predetto requisito sia rispettato anche dai fornitori nell'ipotesi di esternalizzazione di un servizio;

 	Nome documento	Revisione	00
	Politica per la Sicurezza delle Informazioni Parte Generale	Data	03/02/2026
		Creato da	Responsabile Servizi Continuità
		Approvato da	Direzione
		Tipo di documento	Documento Pubblico

INTEGRITÀ: l'informazione deve essere resa disponibile integra a chi ne ha diritto e verificare/accertarsi che il predetto requisito sia rispettato anche dai fornitori nell'ipotesi di esternalizzazione di un servizio;

DISPONIBILITÀ: l'informazione deve essere disponibile quando richiesta dalle persone autorizzate e verificare/accertarsi che il predetto requisito sia rispettato anche dai fornitori nell'ipotesi di esternalizzazione di un servizio.

La Società salvaguarda il capitale investito nel Sistema Informativo in termini di hardware, software, e mantenimento del sistema stesso.

Prendere coscienza dei costi che la Società deve sopportare per le sostituzioni e le manutenzioni conseguenti a cedimenti della sicurezza. La gestione del rischio è eseguita per gli Asset di cui sopra con la seguente metodologia:

- Analisi alto livello del rischio di ogni Assets con le protezioni in atto.
- Individuazione degli Assets che dall'analisi alto livello presentano un valore dell'Asset non trascurabile "compromesso" dal rischio.
- Analisi di dettaglio del rischio su quegli Assets che dall'analisi alto livello presentano un valore dell'Asset compromesso non trascurabile.

Se dall'analisi di dettaglio il livello di rischio rimane non trascurabile, occorre verificare l'efficacia delle protezioni di base e/o introduzione di nuove protezioni dedicate agli specifici Assets.

Per garantire quanto sopra la Società mette in atto e verifica/si accerta che i fornitori mettano in atto le seguenti contromisure:

- Impostazione ed attuazione dei necessari ed adeguati controlli per la difesa da attacchi o incidenti conformemente alle normative in vigore.
- Rendere edotti tutti i lavoratori e collaboratori **implicati** nel Sistema Informativo aziendale e in quelli dei clienti, delle proprie specifiche responsabilità per evitare comportamenti e prassi operative non idonee.
- Impegno del management a perseguire gli obiettivi per la sicurezza.
- Meccanismi per la distribuzione delle autorizzazioni agli accessi fisici e logici e contromisure in caso di violazione.
- Adozione di un sistema di controllo degli accessi.
- Consapevolezza di ogni lavoratore/collaboratore della necessità di operare per salvaguardare le informazioni. A tale scopo, tutti sono addestrati a seguire le regole e le procedure che sono state stabilite e tutti sono soggetti a formazione in tema di sicurezza.
- Introduzione di processi di monitoraggio per valutare l'applicazione e l'efficacia.
- Comunicazione a mezzo web delle politiche e dei KPI adottati a lavoratori.
- Riesame annuale delle politiche attuate.