



Politica di Sicurezza delle
Informazioni (ISP)

Rev. 01
Del 11.07.2025

POLITICA DI SICUREZZA DELLE INFORMAZIONI

Revisione	Data Revisione	Descrizione	Redatto da	Approvato da	Classificazione
01	11.07.2025	Prima Emissione	Lorenzo Corti	Leone Tronconi	Pubblico

PUBBLICO



Politica di Sicurezza delle Informazioni (ISP)

Rev. 01
Del 11.07.2025

Il Sistema di Gestione della Sicurezza delle Informazioni è lo strumento con il quale Timenet S.p.A. intende proteggere la riservatezza, l'integrità, la disponibilità e l'autenticità del proprio patrimonio informativo, ivi incluse le informazioni sensibili dei suoi clienti e fornitori.

Il conseguimento di adeguati livelli di sicurezza consente a Timenet S.p.A. di prevenire, mitigare e contrastare eventi dannosi che potrebbero compromettere la sicurezza delle persone, l'immagine e la reputazione aziendale, nonché di generare impatti negativi di natura economica, finanziaria, legale o operativa. L'adozione di misure efficaci di sicurezza delle informazioni contribuisce inoltre a garantire la conformità ai requisiti contrattuali, normativi e legislativi vigenti, inclusi quelli in materia di protezione dei dati personali, tutela del patrimonio informativo e gestione dei rischi di cybersicurezza.

L'osservanza della presente Politica per la Sicurezza delle Informazioni è obbligatoria per tutto il personale di Timenet S.p.A., inclusi dipendenti, collaboratori, consulenti, fornitori, appaltatori, partner e ogni altra parte esterna che, a qualunque titolo, accede, gestisce o tratta informazioni appartenenti all'Organizzazione o ai suoi clienti. Tali soggetti sono tenuti a rispettare i principi, le regole e le procedure definite, contribuendo attivamente alla protezione del sistema informativo aziendale e al mantenimento della fiducia degli stakeholder.

Obiettivi

La Società mette in pratica questi principi con i seguenti obiettivi:

1. Proteggere gli asset informativi aziendali e dei clienti/fornitori acquisiti, trattati o generati nell'ambito dei servizi erogati, salvaguardando la loro riservatezza, l'integrità, disponibilità ed autenticità;
2. Garantire il corretto accesso ai giusti asset informativi quando necessario e prevenire l'accesso non autorizzato, sia da parte di chi opera in Timenet, sia di chi opera per suo conto;
3. Implementare misure tecniche ed organizzative per ridurre la probabilità e l'impatto degli incidenti informatici, istituendo processi efficaci di monitoraggio, gestione degli eventi e risposta agli incidenti;
4. Definire ruoli e responsabilità interni ed esterni per la sicurezza delle informazioni, in base a specifiche competenze e background professionale;
5. Supportare il personale e i collaboratori con un'adeguata istruzione e formazione per sensibilizzare in materia di sicurezza informatica al fine di minimizzare i rischi, per quanto possibile;
6. Garantire la continuità della sicurezza delle informazioni e dei servizi core in caso di scenario sfavorevole o qualora si concretizzi una minaccia;
7. Assicurare l'adozione del principio di sicurezza sin dalla progettazione (security by design) e per impostazione predefinita (security by default), introducendo specifici requisiti di sicurezza



Politica di Sicurezza delle Informazioni (ISP)

Rev. 01
Del 11.07.2025

fin dalle fasi di progettazione, sviluppo e acquisizione dei sistemi, garantendo che le configurazioni predefinite riducano al minimo i rischi informatici;

8. Mantenere l'osservanza delle disposizioni contrattuali, legislative e regolamentari, in particolare sulla protezione delle informazioni, tra cui la norma ISO/IEC 27001:2022 e il Regolamento (UE) 2024/2690;
9. Garantire un'idonea custodia delle informazioni Personali di terzi e la loro gestione secondo principi di liceità, proporzionalità e pertinenza.

La Società raggiunge gli obiettivi prefissati di sicurezza delle informazioni tramite un approccio di gestione del rischio strutturato e pianificando opportune misure di mitigazione su diversi fronti.

La Direzione di Timenet S.p.A.

- ✓ è direttamente responsabile dell'attuazione della presente Politica e dell'osservanza della stessa da parte di tutte le parti interessate;
- ✓ condivide i principi e gli obiettivi del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) e ne sostiene pienamente la realizzazione e il mantenimento fornendo le risorse necessarie a tale scopo;
- ✓ si impegna a mantenere e rafforzare costantemente il livello di sicurezza dei propri sistemi informativi e di rete, mediante attività di verifica e revisione regolare delle misure adottate; ad intervalli pianificati e/o al manifestarsi di eventi significativi (quali incidenti, cambiamenti operativi o risultati di audit), saranno aggiornati processi, strumenti e configurazioni al fine di garantire una risposta efficace alle nuove minacce e il continuo allineamento con le migliori pratiche e standard internazionali;
- ✓ fornisce le risorse e la formazione continua necessaria al miglioramento nel tempo del SGSI. È direttamente responsabile dell'allocazione delle risorse necessarie - umane, finanziarie, tecnologiche e procedurali - per realizzare le misure di cibersicurezza e sicurezza delle informazioni; ciò comprende personale qualificato, budget dedicati, tecnologie aggiornate, strumenti di monitoraggio e risposta, nonché processi formalizzati per gestire la sicurezza, la formazione periodica e le attività di controllo.



Politica di Sicurezza delle Informazioni (ISP)

Rev. 01
Del 11.07.2025

Ruoli, Responsabilità e Autorità in materia di Sicurezza degli Asset & Sistemi Informativi e di Rete

Ruolo	Responsabilità	Autorità	Riporta a	Ruolo Interno / Esterno
Responsabile della Sicurezza delle Informazioni (CISO - RSGSI)	<ul style="list-style-type: none">- Implementa, monitora, aggiorna e migliora costantemente la compliance di Timenet S.p.A. agli standard e regolamenti internazionali in materia di Sicurezza delle Informazioni;- Monitora gli aspetti di Sicurezza delle informazioni in ogni fase del processo di erogazione del servizio, in collaborazione con i rispettivi Responsabili;- Programma verifiche ispettive interne e/o esterne, al fine di monitorare l'effettiva compliance dell'Organizzazione alle disposizioni normative di riferimento;- Coordina e monitora la presa in carico delle azioni di mitigazione derivanti dalla rilevazione di	Autorità decisionale in materia di misure di sicurezza finalizzate alla protezione del patrimonio informativo dell'Organizzazione.	CdA - Consiglio di Amministrazione	Ruolo Interno e Specifico



Politica di Sicurezza delle Informazioni (ISP)

Rev. 01
Del 11.07.2025

	<p>potenziali gap, verificando la corretta attuazione ed efficacia delle stesse;</p> <ul style="list-style-type: none">- È in diretto contatto con la Direzione, al fine di informarla sull'andamento del livello di Sicurezza delle Informazioni all'interno dell'Azienda;- In collaborazione con Ufficio Risorse Umane, sviluppa e definisce campagne di formazione in materia di information & cyber security;- Gestisce e coordina eventuali incidenti di sicurezza informatica in collaborazione con il Responsabile ICT ed il suo team;- Valuta i rischi strategici in materia di information & cyber security, nonché definisce delle attività minime necessarie per la loro eventuale mitigazione.			
Responsabili ICT / Team ICT	- Gestisce l'infrastruttura tecnologica aziendale,	Autorità in materia di configurazione, controllo,	Amministratore Delegato /	Ruolo Interno



Politica di Sicurezza delle Informazioni (ISP)

Rev. 01
Del 11.07.2025

	<p>garantendo che i sistemi, le reti e gli applicativi siano sicuri, stabili e performanti;</p> <ul style="list-style-type: none">- Gestisce la manutenzione e revisione degli accessi, nonché il ciclo di vita delle identità logiche;- È direttamente coinvolto della definizione di strategie IT, assicurandosi che l'infrastruttura tecnologica sia allineata con gli obiettivi aziendali, supporti la crescita e l'innovazione.	<p>monitoraggio e implementazione delle soluzioni tecniche di sicurezza.</p>	Direzione Operativa	
Direttore Assurance & Provisioning	<ul style="list-style-type: none">- Definisce, coordina e monitora i criteri e le modalità di valutazione dei fornitori aziendali che accedono o trattano direttamente il patrimonio informativo dell'Organizzazione e dei suoi Clienti;- Stabilisce i requisiti minimi, inclusi quelli di natura legale e contrattuale, che tali fornitori sono tenuti a rispettare in materia di	<p>Esercita l'autorità decisionale in merito alla selezione, sospensione o cessazione dei rapporti con fornitori che non soddisfano i requisiti minimi previsti dall'Organizzazione in termini di sicurezza delle informazioni, conformità normativa e</p>	Amministratore Delegato Direzione Operativa	Ruolo Interno



Politica di Sicurezza delle Informazioni (ISP)

Rev. 01
Del 11.07.2025

	sicurezza delle informazioni.	performance contrattuale; opera in autonomia nello sviluppo, nell'adozione e nell'aggiornamento delle metodologie di valutazione e monitoraggio dei fornitori.		
Responsabile della Protezione dei Dati (DPO) / Legal Counsel	- Supervisiona le modalità di trattamento dei dati personali trattati dall'Organizzazione; - Si coordina con il RSGSI per la gestione del Sistema Privacy conforme alla materia GDPR; - Gestisce eventi di Data Breach in collaborazione con la figura del Garante della Privacy ed autorità interessate in materia (Guardia di Finanza, Polizia Postale).	Detiene l'autorità per supervisionare i trattamenti dei dati personali e per definire, validare e monitorare le misure organizzative e tecniche a tutela della protezione dei dati.	Amministratore Delegato Direzione Operativa	DPO: ruolo esterno Legal Counsel: ruolo interno

Con l'obiettivo della massima trasparenza e collaborazione, la presente politica per la Sicurezza delle Informazioni è comunicata a tutti i dipendenti e resa disponibile a tutte le parti interessate per quanto ritenuto necessario dal Management.

La Politica, insieme ai ruoli e alle responsabilità assegnati in materia di Sicurezza delle Informazioni, è soggetta a revisione con cadenza annuale e/o in occasione di cambiamenti significativi che



Politica di Sicurezza delle
Informazioni (ISP)

Rev. 01
Del 11.07.2025

possano incidere sulla sicurezza delle informazioni, al fine di garantirne costantemente l'idoneità, l'adeguatezza e l'efficacia.

Empoli, 11 luglio 2025

La Direzione di TIMENET S.p.A.

Leave Trace