ISO/IEC 27001

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Clausole 5.1-5.2 e controllo A.5.1 - ISO/IEC 27001:2022

di

INNOVENGER S.r.l.

Codice documento	POL-SI-01
Titolo	Politica per la sicurezza delle informazioni
Tipo	Politica del SGSI
Versione	01
Data di emissione	01/10/2026
Responsabile	Pietro D'Ambrosio, CIO e Responsabile SGSI
Approvato da	Claudio Bianchi, Amministratore Delegato
Classificazione	Livello 1 - PUBBLICO
Norme di riferimento	ISO/IEC 27001:2022 (cl. 5.1, 5.2, 6.2, 7.3, 7.4, 9.3; A.5.1), Reg. UE 2016/679 (GDPR), D.Lgs. 196/2003, L. 300/1970
Sostituisce	Information Security Policies v1.1 del 12/03/2026 (in inglese)
Prossima revisione	Ottobre 2027, o prima in caso di cambiamenti significativi

Documento soggetto a revisione annuale. Ogni stampa o copia non aggiornata è da considerarsi non controllata.

INDICE

1. SCOPO 3
2. CAMPO DI APPLICAZIONE 3
3. CONTESTO E FINALITÀ 3
4. PRINCIPI 3
5. IMPEGNI DELLA DIREZIONE 3
5.1 Impegno a soddisfare i requisiti applicabili 3
5.2 Impegno al miglioramento continuo del SGSI 4
6. OBIETTIVI PER LA SICUREZZA DELLE INFORMAZIONI 4
6.1 Obiettivi 2026-2027 4
6.2 Obiettivi di lungo periodo 4
7. RUOLI E RESPONSABILITÀ 4
8. AREE DI CONTROLLO E POLITICHE DI DETTAGLIO 5
9. COMUNICAZIONE E DISPONIBILITÀ 5
10. INDICATORI 6
11. VERIFICA DI CONFORMITÀ E VIOLAZIONI 6
12. ECCEZIONI 6
13. DOCUMENTI COLLEGATI 6
14. RIESAME DELLA POLITICA 6
APPROVAZIONE E FIRME 7
STORICO DELLE REVISIONI 7

1. Scopo

La presente politica è la politica di vertice del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) di INNOVENGER S.r.l., ai sensi della clausola 5.2 e del controllo A.5.1 della ISO/IEC 27001:2022. Definisce principi, impegni della Direzione, quadro degli obiettivi, ruoli e aree di controllo. Le regole operative sono nelle politiche di dettaglio richiamate al capitolo 8.

2. Campo di applicazione

La politica si applica al SGSI con lo scopo di certificazione «Progettazione ed erogazione di servizi e consulenza in ambito software e cybersecurity», che comprende:

- la sede legale di Milano e l'unità locale di Napoli, usate per le riunioni;
- le postazioni di lavoro remoto, da cui il personale svolge tutta l'attività;
- i servizi cloud e SaaS che ospitano le informazioni aziendali e gli ambienti di sviluppo;
- le piattaforme proprietarie di INNOVENGER;
- il trattamento di dati per conto dei clienti e la gestione di siti e applicazioni dei clienti;
- la catena di fornitura dei fornitori critici.

Vale per tutte le informazioni e per chiunque vi acceda.

3. Contesto e finalità

INNOVENGER è una PMI innovativa di consulenza tecnologica, digital transformation e cybersecurity. Opera interamente da remoto, con risorse informatiche in cloud. I clienti le affidano informazioni riservate, accessi ai propri sistemi e dati personali: la sicurezza delle informazioni è parte del servizio, oltre che una condizione per erogarlo. Le priorità del SGSI derivano dall'Analisi del contesto, dall'Analisi delle parti interessate e dalla valutazione dei rischi.

4. Principi

- **Riservatezza, integrità e disponibilità:** le informazioni sono accessibili solo agli autorizzati, restano corrette e sono disponibili quando servono.
- **Approccio basato sul rischio:** le misure derivano dai rischi valutati e sono proporzionate all'organizzazione.
- **Minimo privilegio:** ogni persona accede solo a ciò che serve al proprio ruolo.
- **Identità al centro:** la protezione si basa su identità verificate con autenticazione a più fattori e su dispositivi gestiti dall'azienda.
- **Sicurezza fin dalla progettazione:** i requisiti di sicurezza e protezione dei dati sono definiti all'avvio di ogni progetto o servizio.
- **Separazione dei compiti:** chi attua una modifica rilevante non la approva; le modifiche del Responsabile SGSI sono approvate dall'Amministratore Delegato.
- **Evidenza:** ogni regola produce un'evidenza verificabile (registro, report, verbale).

5. Impegni della Direzione

L'Amministratore Delegato, per conto della Direzione, assume in modo esplicito i due impegni seguenti e assicura le risorse necessarie per attuarli.

5.1 Impegno a soddisfare i requisiti applicabili

INNOVENGER si impegna a soddisfare tutti i requisiti applicabili alla sicurezza delle informazioni:

- **Legali e regolamentari:** in particolare GDPR e D.Lgs. 196/2003, art. 4 della L. 300/1970, norme su documenti informatici e segreto industriale.
- **Contrattuali:** riservatezza, livelli di servizio, requisiti di sicurezza, diritti di audit e accordi sul trattamento dei dati concordati con clienti e fornitori.

- **Delle parti interessate:** le esigenze di clienti, personale, fornitori, ente di certificazione e autorità individuate nell'Analisi delle parti interessate.
- **Volontari:** la ISO/IEC 27001:2022. La Direttiva NIS2 è un riferimento volontario di buona pratica: INNOVENGER non rientra nel suo perimetro.

Il Responsabile SGSI, con la Compliance Specialist, aggiorna i requisiti e ne verifica il rispetto almeno annualmente.

5.2 Impegno al miglioramento continuo del SGSI

INNOVENGER si impegna a migliorare in modo continuo l'idoneità, l'adeguatezza e l'efficacia del SGSI, sulla base di evidenze: indicatori e obiettivi, esiti degli audit, incidenti e non conformità (con azioni correttive registrate nel Registro REG-NC-01), cambiamenti del contesto e delle minacce, segnalazioni di personale, clienti e fornitori. Le decisioni di miglioramento sono verbalizzate nel Riesame della Direzione.

6. Obiettivi per la sicurezza delle informazioni

La presente politica è il quadro per fissare gli obiettivi di sicurezza (clausola 6.2). Ogni obiettivo è misurabile, ha un responsabile e una scadenza. I KPI di dettaglio sono nella tabella degli obiettivi e degli indicatori del SGSI e, per gli obiettivi di lungo periodo, nel Programma PGM-AI-001; lo stato di avanzamento è presentato nel Riesame della Direzione.

6.1 Obiettivi 2026-2027

Obiettivo	Traguardo	Scadenza	Responsabile
Certificazione ISO/IEC 27001:2022	Certificato rilasciato	Dicembre 2026	Amministratore Delegato
Autenticazione a più fattori	100% degli utenti con MFA attiva	Continuo	Responsabile SGSI
Formazione sulla sicurezza	100% del personale formato ogni anno	Annuale	Responsabile SGSI con HR Manager
Non conformità	Zero non conformità maggiori aperte	Continuo	Responsabile SGSI
Prove di ripristino	Prova mensile di ripristino dei siti e prova trimestrale di Microsoft 365, documentate	Mensile e trimestrale	Responsabile SGSI

6.2 Obiettivi di lungo periodo

Codice	Obiettivo	Risultato atteso
OB-1	Asset management completo	Asset informativi, servizi cloud, piattaforme e servizi di terzi censiti con owner e classificazione in un inventario aggiornato.
OB-2	Sviluppo sicuro e conservazione del codice sorgente delle piattaforme proprietarie	Ciclo di sviluppo sicuro su tutte le piattaforme proprietarie; codice sorgente conservato con accessi tracciati e copie recuperabili.
OB-3	Resilienza indipendente dai fornitori critici	Dati e servizi critici ripristinabili anche se un fornitore critico resta a lungo indisponibile.

Gli obiettivi sono riesaminati ogni anno nel Riesame della Direzione.

7. Ruoli e responsabilità

Ruolo	Responsabilità
Amministratore Delegato	Approva politica e obiettivi, assicura le risorse, accetta per iscritto i rischi residui, conduce il Riesame della Direzione. Riferisce al CdA.
CIO e Responsabile SGSI	Ha la delega operativa per la sicurezza delle informazioni: mantiene SGSI e politiche, coordina rischi e incidenti, riceve le segnalazioni, misura gli obiettivi.
Compliance Specialist	Supporta documentazione, requisiti legali e contrattuali e pianificazione degli audit interni; cura registri e prese visione.
Owner di processo e di asset	Indicato nell'Asset Inventory o nella BIA: classifica le informazioni, autorizza gli accessi, segue rischi e controlli del proprio ambito.
Tutto il personale	Firma la presa visione, applica le politiche, completa la formazione, segnala subito (entro 1 ora) incidenti e anomalie al Responsabile SGSI. Chi segnala in buona fede non subisce conseguenze.

Ruolo	Responsabilità
Collaboratori e fornitori	Rispettano la politica e le clausole contrattuali di sicurezza e riservatezza; segnalano senza ritardo gli incidenti.

8. Aree di controllo e politiche di dettaglio

Area	Principio in sintesi	Documento di dettaglio
Gestione del rischio	Valutazione almeno annuale e a ogni cambiamento significativo; controlli motivati nella SoA.	Risk Management 2.7; Registro dei Rischi; SoA
Classificazione e asset	Tre livelli: PUBBLICO, USO INTERNO (default), RISERVATO. Ogni asset ha un owner ed è inventariato.	Classificazione delle informazioni 1.3; Politica di gestione degli asset 2.2
Accessi logici	Account nominali, minimo privilegio, MFA, account amministrativi distinti, riesame periodico, revoca tempestiva alla cessazione.	POL-ACC-01
Cloud e fornitori	Valutazione prima dell'adozione, clausole di sicurezza e accordi sul trattamento dei dati, riesame annuale dei fornitori critici.	POL-CLD-01; Politica sulla sicurezza dei fornitori di terze parti 2.1; Policy di sicurezza dei fornitori critici e della supply chain 2.0
Personale	Verifiche di selezione nei limiti di legge, impegno di riservatezza, formazione all'ingresso e annuale, uso autorizzato dell'intelligenza artificiale.	POL-PER-01; AI Acceptable Use Policy
Sicurezza fisica e lavoro remoto	Nessun dato aziendale nelle sedi; dispositivi gestiti e cifrati; schermo e scrivania puliti; data center protetti dai fornitori cloud.	POL-FIS-01; Politica sulla scrivania e sullo schermo pulito 1.3
Gestione dei sistemi	Configurazione sicura, aggiornamenti, anti-malware, registrazione degli eventi, crittografia, cambiamenti controllati.	System Management Security 1.6 e politiche collegate; PRO-CHG-001
Incidenti	Segnalazione entro 1 ora, registrazione di ogni incidente, analisi delle cause e azioni correttive.	POL-INC-01
Continuità operativa	Processi critici e tempi di ripristino definiti nella BIA; backup e prove di ripristino periodiche.	POL-BCM-01; BIA-01; Policy di backup e ripristino 1.2
Dati personali	Ruolo di Titolare per i propri dati e di Responsabile per i dati dei clienti; protezione fin dalla progettazione; violazioni gestite nei termini del GDPR.	POL-PRV-01
Sviluppo sicuro	Requisiti di sicurezza in ogni progetto, ambienti separati, codice protetto, penetration test annuale sulle applicazioni critiche.	System Management Security 1.6; obiettivo OB-2

9. Comunicazione e disponibilità

La politica è classificata Livello 1 - PUBBLICO e non contiene dettagli interni. Il Responsabile SGSI ne cura la diffusione.

Destinatario	Modalità	Evidenza
Personale	Presa visione firmata all'ingresso, prima dell'attivazione dell'account, e a ogni revisione significativa; disponibile nel repository del SGSI.	Prese visione firmate
Collaboratori e fornitori	Richiamo nei contratti e negli ordini, accettato prima dell'accesso.	Contratto o ordine
Clienti	Richiamo nelle offerte e nei contratti.	Offerte e contratti
Pubblico	Pubblicazione su innovenger.com entro 15 giorni dall'approvazione.	Pagina pubblicata

Richieste di informazioni e segnalazioni di problemi di sicurezza: info@innovenger.com, all'attenzione del Responsabile SGSI.

10. Indicatori

Indicatore	Traguardo	Frequenza	Fonte
Personale con presa visione della versione in vigore	100%	Continua	Registro delle prese visione
Versione sul sito uguale a quella approvata	Sì	Trimestrale	Compliance Specialist
Offerte e contratti con richiamo alla politica	100%	Semestrale, a campione	Compliance Specialist
Obiettivi raggiunti entro la scadenza	100%	Annuale	Riesame della Direzione

11. Verifica di conformità e violazioni

La conformità è verificata con gli audit interni (PRO-AI-001, PGM-AI-001) e con gli audit dell'ente di certificazione. Le non conformità sono registrate nel REG-NC-01. Per il personale le violazioni possono comportare provvedimenti disciplinari proporzionati, secondo il CCNL applicato e l'art. 7 della L. 300/1970; per collaboratori e fornitori si applicano i rimedi contrattuali.

12. Eccezioni

Principi e impegni non ammettono eccezioni. Le eccezioni alle politiche di dettaglio sono richieste per iscritto al Responsabile SGSI, motivate, temporanee e con misure compensative; per rischio alto le approva l'Amministratore Delegato. Sono annotate nel Registro delle eccezioni.

13. Documenti collegati

Documento	Relazione
Analisi del contesto 1.6; Analisi delle parti interessate 1.8	Requisiti e priorità
POL-PER-01, POL-FIS-01, POL-ACC-01, POL-CLD-01, POL-INC-01, POL-PRV-01, POL-BCM-01	Regole di dettaglio
Tabella degli obiettivi e degli indicatori; Programma PGM-AI-001; Riesame della Direzione	KPI, riesame di politica e obiettivi
Registro REG-NC-01; Registro delle eccezioni	Non conformità ed eccezioni

14. Riesame della politica

La politica è riesaminata almeno una volta l'anno nel Riesame della Direzione, e prima in caso di cambiamenti significativi dell'organizzazione, del contesto, dei requisiti o dei rischi, di incidenti rilevanti o di esiti di audit. Il Responsabile SGSI propone le modifiche, l'Amministratore Delegato le approva. Prossima revisione: ottobre 2027.

Approvazione e firme

Con la firma, l'Amministratore Delegato approva la politica e ne dispone la comunicazione alle persone e alle parti interessate indicate.

Ruolo	Nome	Data	Firma
Redatto da – CIO e Responsabile SGSI	Pietro D'Ambrosio		
Approvato da – Amministratore Delegato	Claudio Bianchi		

Storico delle revisioni

Versione	Data	Descrizione
01	01/10/2026	Prima emissione in italiano, riscritta e ampliata sulla realtà di INNOVENGER. Sostituisce: Information Security Policies v1.1 del 12/03/2026 (in inglese).