Codice	Titolo	Revisione	Classificazione
POL-SIC-08	**Politica di sicurezza delle informazioni**	Rev. 00	Pubblico

Rev.	Data	Descrizione modifica	Redatto	Approvato
00	21/07/2026	Prima emissione	A. Conati Barbaro	Stefano Linari

1. SCOPO

Con la presente politica la Direzione di Alleantia S.r.l. dichiara l'impegno a proteggere la riservatezza, l'integrità e la disponibilità delle informazioni che l'organizzazione crea, tratta e custodisce, comprese quelle affidate dai clienti. È il documento di vertice per la sicurezza delle informazioni nel Sistema di Gestione Integrato e il quadro da cui discendono obiettivi, policy specifiche e procedure. Per un'azienda che sviluppa software per l'Industrial Internet of Things e tratta dati industriali dei clienti, la fiducia dipende dalla capacità di proteggere queste informazioni: per questo la politica orienta il sistema verso un approccio basato sul rischio, una responsabilità condivisa e il miglioramento continuo.

2. CAMPO DI APPLICAZIONE

La politica si applica all'intero sistema nel campo di applicazione: **sviluppo, fornitura, installazione e assistenza dei prodotti software Alleantia per l'Industria Digitale (piattaforma Alleantia Industrial Intelligence, AII, e Cloud Portal)** (MAN-SGI-01). Copre la sede operativa di Via G. Malasoma 26, Pisa, il lavoro da remoto, gli asset informativi, i sistemi e i servizi cloud aziendali, tutto il personale interno ed esterno e le terze parti che accedono a informazioni o sistemi.

3. RIFERIMENTI

- ISO/IEC 27001:2022 e Amd 1:2024
- Regolamento (UE) 2016/679 e D.Lgs. 196/2003
- D.Lgs. 138/2024 (NIS2), per i requisiti trasferiti dai clienti della catena di fornitura
- Regolamento (UE) 2024/2847 (Cyber Resilience Act)
- POL-SGI-01; POL-SGI-02; POL-SIC-09

4. RUOLI E RESPONSABILITÀ

Ruolo	Responsabilità
Direzione	Approva la politica, assicura le risorse, accetta i rischi residui e risponde in via finale della sicurezza delle informazioni.
Direttore Operazioni / RSGI	Mantiene aggiornata la politica, ne coordina la diffusione e verifica che controlli, gestione del rischio e obiettivi siano coerenti con essa.
Amministratori di sistema (REG-SIC-03)	Applicano a infrastrutture, sistemi e servizi cloud configurazioni sicure coerenti con la politica.
Tutto il personale	Conosce e rispetta la politica, usa gli asset in modo accettabile e segnala tempestivamente ogni evento di sicurezza osservato o sospetto.

www.alleantia.com

Alleantia s.r.l. www.alleantia.com
Sede legale: Via Tosco Romagnola 136 56025 Pontedera (PI)
Sede operativa: Via G. Malasoma 26 56121 Pisa
Partita IVA/Cod. fiscale 02011550502, Capitale sociale €88.605,69
Tel. (+39) 050/9911933 info@alleantia.com

La ripartizione dettagliata dei compiti di sicurezza è definita in POL-SIC-09.

5. OBIETTIVI DI SICUREZZA DELLE INFORMAZIONI

Gli obiettivi, coerenti con la politica, il contesto e la valutazione dei rischi, nascono principalmente dalle azioni di mitigazione dei rischi e servono a ridurli a livelli accettabili, rafforzare la protezione dei servizi ai clienti e dimostrare la conformità. Coprono in particolare: protezione delle reti e dei sistemi esposti; controllo degli accessi e governo dei fornitori IT; monitoraggio degli eventi e gestione degli incidenti; sviluppo sicuro e gestione delle vulnerabilità; continuità operativa; consapevolezza del personale; protezione dei dati personali e conformità normativa. Ogni obiettivo è misurabile ed è registrato nel Programma di miglioramento con responsabile, azioni, risorse, scadenza e monitoraggio (PRO-SGI-04).

6. PRINCIPI

6.1 **Approccio basato sul rischio.** La valutazione dei rischi è la base di ogni decisione sulla sicurezza delle informazioni (PRO-SGI-09).

6.2 **Conformità.** L'organizzazione soddisfa i requisiti legali, regolamentari e contrattuali sulla sicurezza delle informazioni e sulla protezione dei dati, compresi quelli dei clienti, e ne tiene traccia in REG-SGI-01.

6.3 **Responsabilità condivisa.** La sicurezza è responsabilità di ciascuno; il Codice di condotta (POL-SGI-02) collega il comportamento etico al rispetto delle policy, e la formazione e la sensibilizzazione coinvolgono tutto il personale (PRO-SGI-11).

6.4 **Accesso in base alla necessità.** Ognuno accede a informazioni e sistemi solo nella misura richiesta dalla funzione, con lettura distinta dalla modifica; le autorizzazioni discendono da un'indicazione della Direzione, sono documentate in REG-SIC-04 e riesaminate periodicamente. La protezione per livello di sensibilità segue POL-SIC-07.

6.5 **Uso accettabile.** Informazioni e asset si usano per finalità lavorative (sul PC aziendale è ammesso un uso personale limitato, con i soli programmi installati dall'organizzazione: POL-SIC-10 §8), nel rispetto delle norme e delle regole aziendali; chi riceve un asset ne prende carico formalmente (modulo di assegnazione). Le regole di dettaglio sono in POL-SIC-01 e nella POL-SIC-10; il ciclo di vita degli asset nella PRO-SIC-05 e in POL-SIC-04.

6.6 **Scrivania pulita e schermo pulito.** I documenti riservati non restano incustoditi su scrivanie o stampanti condivise; le postazioni non presidiate sono bloccate e i dispositivi si bloccano automaticamente dopo un periodo di inattività; gli schermi non espongono informazioni riservate a terzi. L'efficacia si verifica con i test di sicurezza fisica (PRO-SIC-02).

6.7 **Segnalazione degli eventi.** Il personale segnala tempestivamente alla Direzione, via email o telefono, ogni evento di sicurezza osservato o sospetto (MOD-SIC-03); ogni incidente, anche se risolto subito, si registra in REG-SIC-01. La segnalazione in buona fede è incoraggiata e non ha conseguenze per chi la fa.

6.8 **Miglioramento continuo.** Nel riesame della direzione (PRO-SGI-03) la Direzione esamina gli esiti della valutazione dei rischi, degli audit, del monitoraggio degli obiettivi, delle verifiche dei controlli e degli incidenti.

www.alleantia.com

Sede legale: Via Tosco Romagnola 136 56025 Pontedera (PI)
Sede operativa: Via G. Malasoma 26 56121 Pisa
Partita IVA/Cod. fiscale 02011550502, Capitale sociale €88.605,69
Tel. (+39) 050/9911933 info@alleantia.com

7. PROTEZIONE DEGLI ASSET FUORI SEDE

Le informazioni e i dispositivi aziendali si proteggono anche fuori sede, in particolare nel lavoro agile e presso i clienti. I dispositivi assegnati sono configurati e mantenuti dall'organizzazione con i soli programmi necessari e con le protezioni previste (disco cifrato, Sophos). In particolare:

- il lavoro da remoto si svolge nei luoghi concordati negli accordi di lavoro agile; nei luoghi pubblici si evita di trattare informazioni riservate dove lo schermo o le conversazioni sono accessibili a terzi;
- in lavoro agile e nei luoghi pubblici qualsiasi attività si svolge con la VPN aziendale attiva, sia per i sistemi interni sia per i servizi cloud, che si usano comunque con credenziali personali e autenticazione a più fattori;
- dispositivi e software aziendali si usano secondo le regole di uso accettabile e non si affidano ad altre persone;
- i dispositivi si custodiscono per prevenirne smarrimento, furto e accesso non autorizzato, senza lasciarli incustoditi;
- guasti, smarrimenti, furti o danneggiamenti si segnalano subito e si trattano come eventi di sicurezza;
- alla cessazione o al cambio di ruolo tutti i beni si restituiscono con il modulo di restituzione.

8. COMUNICAZIONE E RIESAME

La politica è comunicata a tutto il personale all'emissione e a ogni revisione, con presa visione (MOD-SGI-01), e resa disponibile su richiesta alle parti interessate esterne pertinenti, insieme a POL-SGI-01. Il Direttore Operazioni / RSGI la riesamina almeno una volta l'anno e a ogni cambiamento significativo di organizzazione, servizi, tecnologia, requisiti o rischi; la Direzione approva ogni revisione.

www.alleantia.com

Sede legale: Via Tosco Romagnola 136 56025 Pontedera (PI)
Sede operativa: Via G. Malasoma 26 56121 Pisa
Partita IVA/Cod. fiscale 02011550502, Capitale sociale €88.605,69
Tel. (+39) 050/9911933 info@alleantia.com