					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: PII14					Titolo del documento: **Politica di sicurezza e controllo degli accessi PII**							
Versione: 1.0		Data di entrata in vigore: 01.01.2025			Proprietario del documento:							
X	Politica		Standard		Procedura		Modulo		Registro		Altro	

Cronologia delle revisioni				
Numero di revisione	**Data di revisione**	**Modifiche**	**Riesaminato da**	**Proprietario del processo**

Approvazioni			
Nome	**Ruolo**	**Data**	**Firma**

Allineamento a standard e normative applicabili

Standard / Regolamento	Clausola / Controllo / Articolo	Applicabilità	Tipo di copertura	Commento
ISO/IEC 27701:2025	Clause 6.1.3; Clause 8.1	Both	Primary	Pianificazione e operatività dei controlli di sicurezza PII
ISO/IEC 27701:2025	Clause 7.5; Clause 9.1; Clause 10.2	Both	Supporting	Evidenze, monitoraggio e azioni correttive
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9	Both	Primary	Identità e diritti di accesso per il trattamento delle PII
ISO/IEC 27701:2025	Annex A.3.22; Annex A.3.23	Both	Primary	Protezione degli endpoint e autenticazione sicura
ISO/IEC 27701:2025	Annex A.3.25; Annex A.3.26	Both	Primary	Logging e protezione crittografica
ISO/IEC 27701:2025	Annex A.3.28; Annex A.3.29	Both	Supporting	Sicurezza delle applicazioni e architettura sicura
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.15; Annex A.3.16	Both	Supporting	Protezione e riesame delle registrazioni
GDPR	Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32	Both	Primary	Sicurezza, responsabilizzazione e controlli sui responsabili del trattamento
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Integrazione dei controlli ISMS
ISO/IEC 27002:2022	Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Linee guida per l’attuazione dei controlli di sicurezza
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Principi di sicurezza delle informazioni e conformità privacy

ISO/IEC 29151:2022	Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Controlli di sicurezza per la protezione delle PII

1. Ambito di applicazione

1.1 La presente politica definisce i requisiti di sicurezza e di controllo degli accessi specifici per le PII per sistemi, applicazioni, servizi, dispositivi, ambienti cloud e processi operativi che archiviano, trasmettono, trattano, accedono a, amministrano o proteggono PII.

1.2 La presente politica si applica ai contesti di titolare del trattamento, contitolare del trattamento, responsabile del trattamento e sub-responsabile nei quali l'organizzazione determina, gestisce, supporta o si affida a controlli di sicurezza per il trattamento delle PII.

1.3 La presente politica copre i seguenti domini dei controlli di sicurezza PII:

1.3.1 baseline di sicurezza per i dati personali e integrazione con le politiche di sicurezza delle informazioni esistenti;

1.3.2 controllo degli accessi;

1.3.3 autenticazione;

1.3.4 accesso privilegiato;

1.3.5 cifratura e archiviazione sicura;

1.3.6 logging e monitoraggio;

1.3.7 configurazione sicura e gestione delle vulnerabilità;

1.3.8 controlli di accesso per endpoint e cloud;

1.3.9 collegamento delle evidenze tramite REG02, REG08, REG10 e REG12.

1.4 La presente politica non sostituisce un sistema completo di gestione della sicurezza delle informazioni, una politica di sicurezza della rete, una politica di sviluppo sicuro, una politica di backup, una politica sugli endpoint, una politica di sicurezza cloud, uno standard crittografico, una procedura di gestione delle vulnerabilità o una procedura di risposta agli incidenti. Quando tali politiche esistono già, la presente politica definisce i collegamenti specifici per le PII e i requisiti di evidenza necessari per l'assurance del PIMS.

1.5 La presente politica non duplica:

1.5.1 la titolarità dell'inventario dei trattamenti PII e della base giuridica in PII03;

1.5.2 la metodologia di rischio privacy e DPIA in PII07;

1.5.3 i gate di privacy by design in PII08;

1.5.4 le regole di raccolta, utilizzo, comunicazione e condivisione in PII09;

1.5.5 l'esecuzione di conservazione, cancellazione e smaltimento in PII10;

1.5.6 la governance del ciclo di vita dei responsabili del trattamento in PII12;

1.5.7 i controlli sugli strumenti di trasferimento internazionale in PII13;

1.5.8 il workflow per incidenti e violazioni in PII15;

1.5.9 la governance delle informazioni documentate in PII17;

1.5.10 la governance del monitoraggio, dell'audit e del miglioramento del PIMS in PII18.

1.6 Ai fini della presente politica, i log operativi, gli output degli strumenti di sicurezza, le esportazioni dei riesami degli accessi, i report sulle vulnerabilità e le evidenze di configurazione sono fonti di evidenza allegate, sintetizzate o richiamate dagli oggetti di evidenza canonici. Non costituiscono registri PIMS separati.

2. Finalità

2.1 La finalità della presente politica è garantire che le PII siano protette da controlli di sicurezza e di accesso adeguati, allineati al rischio e verificabili in sede di audit durante l'intero trattamento.

2.2 La presente politica consente all'organizzazione di dimostrare che i controlli di sicurezza PII sono pianificati, attuati, riesaminati, monitorati e migliorati tramite REG02, REG08, REG10 e REG12,

senza creare registri di sicurezza duplicati né sostituire le politiche di sicurezza delle informazioni esistenti.

3. Obiettivi

3.1 Gli obiettivi della presente politica sono:

3.1.1 definire una baseline di controllo degli accessi PII per sistemi e attività di trattamento;

3.1.2 garantire che i controlli di autenticazione siano adeguati alla sensibilità delle PII e al contesto di accesso;

3.1.3 definire i requisiti di riesame per l'accesso privilegiato e ordinario alle PII;

3.1.4 definire le aspettative di cifratura e archiviazione sicura per le PII a riposo, in transito e nei pertinenti contesti cloud o endpoint;

3.1.5 definire le aspettative di logging e monitoraggio per l'accesso alle PII, le modifiche alle PII e l'amministrazione delle PII;

3.1.6 definire i requisiti di evidenza per la configurazione sicura e le vulnerabilità dei sistemi che trattano PII;

3.1.7 definire le aspettative di accesso per endpoint e cloud senza creare una politica completa di sicurezza degli endpoint o del cloud;

3.1.8 collegare gli incidenti di sicurezza PII sospetti a REG10 senza duplicare il workflow degli incidenti;

3.1.9 integrarsi con le politiche di sicurezza delle informazioni esistenti, ove disponibili;

3.1.10 mantenere evidenze pronte per l'audit utilizzando esclusivamente REG02, REG08, REG10 e REG12.

4. Dichiarazioni della politica

4.1 Baseline di sicurezza per i dati personali e integrazione con ISMS

4.1.1 [Both] Information Security Lead DEVE definire in REG12 la baseline di sicurezza per i dati personali per ciascun sistema o servizio che tratta PII prima che il sistema o servizio entri in produzione o subisca modifiche sostanziali.

4.1.2 [Both] System Owner / Application Owner DEVE registrare in REG12 la posizione delle evidenze dei controlli di sicurezza PII attuati prima di fare affidamento su un controllo di sicurezza delle informazioni esistente ai fini dell'assurance del PIMS.

4.1.3 [Controller] Process Owner / Business Owner DEVE identificare in REG02 la sensibilità delle PII, il contesto del trattamento e la necessità di accesso prima di richiedere un accesso nuovo o modificato in modo sostanziale alle PII.

4.1.4 [Processor] Vendor / Procurement Owner DEVE registrare in REG08 le istruzioni di sicurezza del cliente, i confini delle responsabilità del cliente e gli impegni di sicurezza del responsabile del trattamento prima che inizi o cambi in modo sostanziale l'accesso del responsabile del trattamento alle PII del cliente.

4.1.5 [Both] Privacy Lead / PIMS Manager DEVE verificare che le evidenze di sicurezza PII siano collegate a REG02, REG08, REG10 o REG12 prima di accettare l'attività di trattamento come verificabile ai fini del PIMS.

4.2 Baseline di controllo degli accessi

4.2.1 [Both] System Owner / Application Owner DEVE limitare l'accesso alle PII ai ruoli approvati e agli utenti autorizzati registrati o tracciabili in REG02 o REG12 prima dell'abilitazione dell'accesso.

4.2.2 [Both] Process Owner / Business Owner DEVE approvare in REG02 o REG12 la finalità aziendale dell'accesso alle PII prima che System Owner / Application Owner effettui il provisioning dell'accesso.

4.2.3 [Both] System Owner / Application Owner DEVE riesaminare almeno trimestralmente gli accessi degli utenti ai sistemi che trattano PII ad alto impatto o sensibili e registrare l'esito del riesame in REG12.

4.2.4 [Both] System Owner / Application Owner DEVE riesaminare almeno annualmente gli accessi degli utenti agli altri sistemi che trattano PII e registrare l'esito del riesame in REG12.

4.2.5 [Both] System Owner / Application Owner DEVE rimuovere o modificare l'accesso alle PII in REG12 entro un giorno lavorativo dal cambio di ruolo, dalla cessazione, dal completamento del contratto o dal venir meno della necessità dell'accesso.

4.2.6 [Processor] Vendor / Procurement Owner DEVE confermare in REG08 che l'accesso del responsabile del trattamento alle PII del cliente è limitato alle istruzioni documentate del cliente prima che l'accesso sia abilitato o modificato.

4.2.7 [Subprocessor] Vendor / Procurement Owner DEVE confermare in REG08 che l'accesso del sub-responsabile alle PII è limitato alle attività di sub-trattamento autorizzate prima che l'accesso del sub-responsabile sia abilitato o modificato.

[... Le sezioni 4.3–8 non sono incluse in questa anteprima. Acquistare il documento completo per accedere all'intero contenuto. ...]

9. Eccezioni

9.1.1 [Both] Information Security Lead DEVE registrare in REG12 ogni eccezione a un requisito di sicurezza PII o di controllo degli accessi prima dell'attivazione dell'eccezione.

9.1.2 [Both] Data Protection Officer / Privacy Advisor DEVE fornire consulenza sulle eccezioni di sicurezza PII a rischio più elevato in REG12 prima dell'approvazione.

9.1.3 [Both] Top Management DEVE approvare in REG12 le eccezioni di sicurezza PII prima dell'attivazione quando l'eccezione riguarda PII ad alto impatto, PII sensibili, accesso privilegiato, cifratura, logging o vulnerabilità ad alto rischio irrisolte.

9.1.4 [Both] Information Security Lead DEVE definire in REG12 la scadenza dell'eccezione, il controllo compensativo e la data di riesame prima dell'approvazione dell'eccezione.

9.1.5 [Both] System Owner / Application Owner DEVE porre rimedio, rinnovare o chiudere in REG12 le eccezioni di sicurezza PII scadute entro cinque giorni lavorativi dalla scadenza.

9.1.6 [Processor] Vendor / Procurement Owner DEVE registrare in REG08 e REG12 le eccezioni di sicurezza del responsabile del trattamento o del sub-responsabile che interessano le PII del cliente prima dell'accettazione.

10. Applicazione della politica

10.1.1 [Both] Privacy Lead / PIMS Manager DEVE registrare in REG12 le non conformità relative a evidenze di sicurezza PII mancanti o incomplete entro cinque giorni lavorativi dall'identificazione.

10.1.2 [Both] Information Security Lead DEVE assegnare in REG12 la titolarità della remediation per i fallimenti dei controlli di sicurezza PII entro cinque giorni lavorativi dalla validazione.

10.1.3 [Both] System Owner / Application Owner DEVE disabilitare o limitare l'accesso alle PII non autorizzato, eccessivo o non supportato entro un giorno lavorativo dalla validazione e registrare l'azione in REG12.

10.1.4 [Conditional] Incident Response Coordinator DEVE collegare le azioni di applicazione a REG10 entro un giorno lavorativo quando la questione riguarda un incidente PII sospetto o confermato.

10.1.5 [Both] Top Management DEVE riesaminare in REG12 le non conformità di sicurezza PII ripetute o ad alto rischio prima del riesame della direzione.

11. Riesame e mantenimento

11.1.1 [All] Privacy Lead / PIMS Manager DEVE riesaminare la presente politica con Information Security Lead almeno annualmente e registrare l'esito del riesame in REG12.

11.1.2 [Both] Information Security Lead DEVE riesaminare la baseline di sicurezza per i dati personali in REG12 entro 30 giorni da una modifica sostanziale tecnologica, delle minacce, di audit, di incidente o normativa che incida sulla sicurezza PII.

11.1.3 [Both] System Owner / Application Owner DEVE aggiornare in REG12 le evidenze di sicurezza PII a livello di sistema entro 30 giorni da una modifica sostanziale di architettura, accessi, configurazione, vulnerabilità o logging.

11.1.4 [Processor] Vendor / Procurement Owner DEVE riesaminare in REG08 le evidenze relative alle responsabilità di sicurezza PII di responsabili del trattamento e sub-responsabili entro 30 giorni da una modifica sostanziale del servizio, delle istruzioni del cliente o del sub-responsabile.

11.1.5 [All] Internal Audit / Compliance Reviewer DEVE verificare le evidenze di riesame della politica e le evidenze selezionate dei controlli di sicurezza PII in REG12 secondo il piano di audit approvato.

12. Politiche correlate

12.1 La presente politica deve essere letta congiuntamente a:

12.2 PII01 - Politica del Sistema di gestione delle informazioni sulla privacy;

12.3 PII02 - Politica su ruoli, responsabilità e accountability privacy;

12.4 PII03 - Politica sull'inventario dei trattamenti PII e sulla base giuridica;

12.5 PII07 - Politica di valutazione del rischio privacy e DPIA;

12.6 PII08 - Politica di privacy by design e by default;

12.7 PII09 - Politica di raccolta, utilizzo, comunicazione e condivisione delle PII;

12.8 PII10 - Politica di conservazione, cancellazione e smaltimento delle PII;

12.9 PII12 - Politica di gestione privacy di responsabili del trattamento, sub-responsabili e terze parti;

12.10 PII13 - Politica sui trasferimenti internazionali di PII;

12.11 PII15 - Politica di gestione degli incidenti e delle violazioni PII;

12.12 PII16 - Politica di formazione, sensibilizzazione e competenza privacy;

12.13 PII17 - Politica di gestione delle informazioni documentate e delle evidenze del PIMS;

12.14 PII18 - Politica di monitoraggio, audit e miglioramento del PIMS.

13. Standard e quadri di riferimento

13.1 ISO/IEC 27701:2025 - Clause 6.1.3; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.7; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5; 5.1.4; 5.1.6; 6.1.2; 7.1.1; 7.1.2].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.5.5; 4.6.3; 4.6.4; 4.7.5; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 7.1.3; 7.1.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.2; 11.1.1; 11.1.5].

13.3 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 10.1.3].

13.4 ISO/IEC 27701:2025 - Annex A.3.22; Annex A.3.23. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5].

13.5 ISO/IEC 27701:2025 - Annex A.3.25; Annex A.3.26. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.6 ISO/IEC 27701:2025 - Annex A.3.28; Annex A.3.29. Addressed by clauses [4.1.1; 4.1.2; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 7.1.1; 7.1.2].

13.7 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.15; Annex A.3.16. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.6.2; 4.6.3; 4.6.4; 4.7.2; 4.7.3; 5.1.9; 6.1.6; 8.1.4; 10.1.1; 11.1.5].

13.8 GDPR - Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.5; 4.2.6; 4.2.7; 4.3.2; 4.4.4; 4.5.1; 4.5.2; 4.6.1; 4.6.6; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 4.8.5; 5.1.1; 5.1.7; 6.1.4; 7.1.4; 9.1.3; 10.1.4].

13.9 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.10 ISO/IEC 27002:2022 - Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.11 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.1; 4.5.1; 4.6.2; 4.6.6; 4.7.6; 5.1.2; 6.1.1; 8.1.4; 10.1.1; 11.1.1].

13.12 ISO/IEC 29151:2022 - Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.7.1; 4.7.2; 4.7.4; 4.8.1; 4.8.2; 6.1.6; 11.1.5].