					Insert Registered Legal Entity Name Here							
Document number: PII17					Document Title: **PIMS Documented Information and Evidence Management Policy**							
Version: 1.0		Effective Date: 01.01.2025			Document Owner:							
X	Policy		Standard		Procedure		Form		Register		Other	

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**

Approvals			
Name	**Title**	**Date**	**Signature**

Aligned with standards and regulations

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 6.1.3	Both	Supporting	SoA documented information
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	PIMS documented information
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Operational evidence control
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Monitoring evidence
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Audit evidence
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Management review evidence
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Nonconformity and corrective action evidence
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Controller processing records
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Processor agreement and instruction evidence
ISO/IEC 27701:2025	Annex A.3.14	Both	Primary	Protection of records
GDPR	Article 5(2)	Controller	Supporting	Accountability evidence
GDPR	Article 24	Controller	Supporting	Controller measures and evidence
GDPR	Article 28	Both	Supporting	Processor documentation
GDPR	Article 30	Both	Supporting	Processing records
GDPR	Article 32	Both	Supporting	Evidence protection
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Privacy compliance evidence
ISO/IEC 29151:2022	Clause 18.1.4	Both	Supporting	Protection of records
ISO/IEC 27001:2022	Clause 7.5	Both	Supporting	Documented information control

ISO/IEC 27002:2022	Control 5.33	Both	Supporting	Protection of records
ISO/IEC 27002:2022	Control 5.34	Both	Supporting	Privacy and PII protection

1. Scope

1.1 This policy defines mandatory requirements for creating, approving, versioning, protecting, retaining, retrieving, translating, withdrawing, and evidencing PIMS documented information.

1.2 This policy applies to PIMS policies, registers, documented approvals, evidence records, audit evidence, management review records, corrective action evidence, and controlled translations used to demonstrate PIMS conformity.

1.3 This policy applies to controller, joint controller, processor, and subprocessor contexts.

1.4 This policy does not create a separate document-control register. Documented information control evidence is maintained through the canonical PIMS evidence objects REG01 through REG12, with REG03 and REG12 used for control applicability, audit, nonconformity, corrective action, and improvement evidence.

2. Purpose

2.1 The purpose of this policy is to ensure that PIMS documented information is accurate, controlled, accessible to authorized users, protected against unauthorized change or disclosure, retained for auditability, and withdrawn when obsolete.

2.2 This policy supports certification readiness by ensuring that evidence needed to demonstrate PIMS conformity can be located, verified, retrieved, and linked to applicable policies, controls, processing activities, risks, audits, and corrective actions.

3. Objectives

3.1 The objectives of this policy are to:

3.1.1 define PIMS documented information control requirements;

3.1.2 maintain evidence integrity across REG01 through REG12;

3.1.3 ensure policy and evidence approval is traceable;

3.1.4 ensure version history and withdrawal decisions are documented;

3.1.5 link PIMS evidence to the Statement of Applicability and policy mappings;

3.1.6 control access to PIMS documents and evidence records;

3.1.7 support multilingual policy and evidence version control;

3.1.8 enable timely retrieval of audit evidence;

3.1.9 prevent unnecessary document-control bureaucracy;

3.1.10 preserve audit-ready records for certification, customer assurance, and continual improvement.

4. Policy Statements

4.1 PIMS documented information control

4.1.1 [All] The Privacy Lead / PIMS Manager MUST maintain a PIMS documented information index in REG12 before initial PIMS publication and quarterly thereafter.

4.1.2 [All] The Process Owner / Business Owner MUST identify documented information required for each owned PII processing activity in REG02 before the processing activity begins and annually thereafter.

4.1.3 [All] The Privacy Lead / PIMS Manager MUST link applicable PIMS policies, controls, and evidence obligations to REG03 before each policy release and within 15 business days of any material control applicability change.

4.1.4 [All] The Privacy Lead / PIMS Manager MUST assign an access level and evidence sensitivity classification to each PIMS documented information category in REG12 before the category is used.

4.2 Creation, approval, versioning, and publication

4.2.1 [All] The Privacy Lead / PIMS Manager MUST assign a document identifier, owner, version number, approval status, effective date, and review date in REG12 before publishing PIMS documented information.

4.2.2 [All] Top Management MUST approve core PIMS policies and material policy changes in REG12 before publication.

4.2.3 [All] The Privacy Lead / PIMS Manager MUST approve PIMS evidence templates or embedded register sections in REG12 before operational use.

4.2.4 [All] The Privacy Lead / PIMS Manager MUST record version history and change rationale in REG12 before releasing updated PIMS documented information.

4.2.5 [All] The Privacy Lead / PIMS Manager MUST record communication of approved PIMS documented information changes in REG11 within 30 days of publication.

[... Sections 4.3–8 are not included in this preview. Purchase the full document to access the complete policy content. ...]

9. Exceptions

9.1.1 [All] The Process Owner / Business Owner MUST request documented information or evidence-control exceptions in REG12 before deviating from this policy.

9.1.2 [All] The Privacy Lead / PIMS Manager MUST assess each documented information or evidence-control exception in REG12 within 10 business days of request.

9.1.3 [All] The Data Protection Officer / Privacy Advisor MUST record advice in REG12 before approval of any exception involving PII evidence disclosure, translation discrepancy, retention conflict, or audit evidence limitation.

9.1.4 [All] Top Management MUST approve documented information exceptions exceeding 30 days or affecting certification, high-risk processing, or external assurance in REG12 before the exception takes effect.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST set an expiry date not exceeding 90 days in REG12 for each approved documented information or evidence-control exception.

9.1.6 [All] The Privacy Lead / PIMS Manager MUST close or reassess each documented information or evidence-control exception in REG12 within five business days of expiry.

10. Enforcement

10.1.1 [All] The Privacy Lead / PIMS Manager MUST record missing, inaccurate, uncontrolled, obsolete, or unretrievable PIMS documented information as a nonconformity in REG12 within five business days of identification.

10.1.2 [All] The Privacy Lead / PIMS Manager MUST prevent publication of PIMS documented information when required approval, version, owner, or effective date evidence is missing from REG12.

10.1.3 [All] The Process Owner / Business Owner MUST prevent audit submission of processing evidence where required owner, date, status, or approval evidence is missing from REG02.

10.1.4 [All] The System Owner / Application Owner MUST remove unauthorized access to PIMS documented information repositories and record the removal in REG12 within one business day of identification.

10.1.5 [All] The Internal Audit / Compliance Reviewer MUST verify corrective action effectiveness for documented information nonconformities in REG12 at the next scheduled audit or within 60 days of closure, whichever occurs first.

11. Review and Maintenance

11.1.1 [All] The Privacy Lead / PIMS Manager MUST review this policy annually and within 30 days of material change to PIMS documented information requirements.

11.1.2 [All] The Privacy Lead / PIMS Manager MUST review this policy within 30 days after a major audit finding, certification nonconformity, repository platform change, or multilingual publication process change.

11.1.3 [All] The Data Protection Officer / Privacy Advisor MUST review privacy-significant changes to this policy in REG12 before approval.

11.1.4 [All] Top Management MUST approve material changes to this policy in REG12 before publication.

11.1.5 [All] The Privacy Lead / PIMS Manager MUST record communication of approved changes to this policy in REG11 within 30 days of publication.

12. Related Policies

12.1 This policy is supported by the following related policies:

12.2 PII01 - Privacy Information Management System Policy

12.3 PII02 - Privacy Roles, Responsibilities and Accountability Policy

12.4 PII03 - PII Processing Inventory and Lawful Basis Policy

12.5 PII04 - Privacy Notice and Transparency Policy

12.6 PII05 - Consent and Preference Management Policy

12.7 PII06 - PII Principal Rights Management Policy

12.8 PII07 - Privacy Risk Assessment and DPIA Policy

12.9 PII08 - Privacy by Design and Default Policy

12.10 PII09 - PII Collection, Use, Disclosure and Sharing Policy

12.11 PII10 - PII Retention, Deletion and Disposal Policy

12.12 PII11 - PII Accuracy and Quality Policy

12.13 PII12 - Processor, Subprocessor and Third-Party Privacy Management Policy

12.14 PII13 - International PII Transfer Policy

12.15 PII14 - PII Security and Access Control Policy

12.16 PII15 - PII Incident and Breach Management Policy

12.17 PII16 - Privacy Training, Awareness and Competence Policy

12.18 PII18 - PIMS Monitoring, Audit and Improvement Policy

13. Reference Standards and Frameworks

13.1 This policy is mapped to the following standards and regulations. The mapping explains how the policy supports the cited requirements and identifies the internal clauses that implement or support them.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.3** - Mapped to maintaining the PIMS Statement of Applicability, control applicability records, and policy-to-evidence linkage. Addressed by clauses [4.1.3; 4.3.3; 6.1.3; 7.1.2].

13.2.2 **Clause 7.5** - Mapped to documented information identification, approval, version control, access, retrieval, preservation, withdrawal, translation version linkage, and retention metadata. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.5; 4.4.1; 4.4.2; 4.4.4; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.1; 4.6.2; 4.6.3; 4.6.4].

13.2.3 **Clause 8.1** - Mapped to operational planning and control evidence for processing records, evidence templates, operational evidence quality, and externally provided evidence. Addressed by clauses [4.1.2; 4.2.3; 4.3.2; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1** - Mapped to maintaining documented evidence of measurement, retrieval performance, evidence gaps, translation mismatches, and repository access review completion. Addressed by clauses [8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6].

13.2.5 **Clause 9.2** - Mapped to audit evidence retrieval, audit sampling, audit evidence traceability, and audit findings related to documented information control. Addressed by clauses [4.3.4; 4.4.4; 6.1.3; 8.1.3; 10.1.5].

13.2.6 **Clause 9.3** - Mapped to management review evidence, management review consideration of documented information control, and Top Management review of evidence-control performance. Addressed by clauses [6.1.2; 8.1.1; 8.1.2; 11.1.4].

13.2.7 **Clause 10.2** - Mapped to documented information nonconformities, corrective action, exception handling, closure, and effectiveness verification. Addressed by clauses [4.3.4; 6.1.4; 9.1.1; 9.1.2; 9.1.4; 9.1.5; 9.1.6; 10.1.1; 10.1.5].

13.2.8 **Annex A.1.2.9** - Mapped to controller processing records, accountability records, processing evidence quality, and retention of evidence supporting controller obligations. Addressed by clauses [4.1.2; 4.3.2; 4.5.1; 7.1.3].

13.2.9 **Annex A.2.2.2** - Mapped to processor agreement, customer instruction, externally provided evidence, and processor relationship evidence control. Addressed by clauses [5.1.7; 7.1.4].

13.2.10 **Annex A.3.14** - Mapped to protection of PIMS records against loss, unauthorized change, unauthorized access, unauthorized release, and improper disposal. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.2; 4.5.4; 4.5.5; 10.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapped to accountability evidence, evidence traceability, evidence retrieval, nonconformity records, and audit-ready records demonstrating compliance. Addressed by clauses [4.1.1; 4.3.2; 4.3.3; 4.4.4; 4.5.4; 6.1.3; 8.1.3; 10.1.1].

13.3.2 **Article 24** - Mapped to controller governance evidence, approval records, policy control, accountability measures, documented review, and Top Management oversight. Addressed by clauses [4.2.2; 4.3.3; 6.1.2; 9.1.4; 11.1.4].

13.3.3 **Article 28** - Mapped to processor and subprocessor documentation, customer instruction evidence, externally provided process evidence, and evidence disclosure control. Addressed by clauses [4.4.5; 5.1.7; 7.1.4].

13.3.4 **Article 30** - Mapped to processing record evidence, evidence quality requirements, processing activity references, and processing evidence owner/status metadata. Addressed by clauses [4.1.2; 4.3.2; 7.1.3; 10.1.3].

13.3.5 **Article 32** - Mapped to protection of evidence repositories, access restrictions, access approvals, repository protection review, and unauthorized access removal. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Mapped to privacy compliance evidence, audit evidence retrieval, evidence traceability, independent review support, and corrective action evidence. Addressed by clauses [4.3.3; 4.4.4; 4.6.3; 6.1.3; 8.1.3; 10.1.5].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.1.4** - Mapped to protection of PII-related records, preservation of records, and evidence repository access and deletion controls. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.5.2; 4.5.5; 10.1.4].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 7.5** - Mapped to documented information identification, approval, availability, protection, version control, retention, disposition, and externally required documented information control. Addressed by clauses [4.1.1; 4.2.1; 4.2.4; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.6.4].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.33 - Mapped to protecting PIMS records against loss, destruction, falsification, unauthorized access, unauthorized release, and improper disposal. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.7.2 Control 5.34 - Mapped to protecting privacy and PII in documented information, evidence repositories, disclosures, and access-controlled records. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 6.1.5].