					Insert Registered Legal Entity Name Here							
Document number: PII01					Document Title: **Privacy Information Management System 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 4.1	Both	Primary	Context and PIMS role determination
ISO/IEC 27701:2025	Clause 4.2	Both	Primary	Interested parties and requirements
ISO/IEC 27701:2025	Clause 4.3	Both	Primary	PIMS scope
ISO/IEC 27701:2025	Clause 4.4	Both	Primary	PIMS establishment and improvement
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Leadership and commitment
ISO/IEC 27701:2025	Clause 5.2	Both	Primary	Privacy policy
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Roles and authorities
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	Risks and opportunities
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Privacy risk assessment
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Privacy risk treatment and SoA
ISO/IEC 27701:2025	Clause 6.2	Both	Primary	Privacy objectives
ISO/IEC 27701:2025	Clause 6.3	Both	Primary	Planned PIMS changes
ISO/IEC 27701:2025	Clause 7.1	Both	Primary	Resources
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Competence
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Awareness
ISO/IEC 27701:2025	Clause 7.4	Both	Primary	Communications
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Documented information
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Operational planning and control

ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Operational privacy risk assessment
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Operational privacy risk treatment
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Monitoring and evaluation
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Internal audit
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Management review
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Continual improvement
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Nonconformity and corrective action
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9	Controller	Primary	Controller governance records
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3	Processor	Primary	Processor agreement and purposes
ISO/IEC 27701:2025	Annex A.3.3	Both	Primary	PII security policy linkage
GDPR	Article 5(2)	Controller	Supporting	Accountability evidence
GDPR	Article 24	Controller	Supporting	Controller measures and policy
GDPR	Article 26	Joint Controller	Supporting	Joint controller arrangements
GDPR	Article 28	Both	Supporting	Processor governance
GDPR	Article 30	Both	Supporting	Processing records
GDPR	Article 32	Both	Supporting	Security of processing
GDPR	Article 35	Controller	Supporting	DPIA governance
ISO/IEC 29100:2020	Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12	Both	Supporting	Privacy controls and principles
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	PIA process and preparation

ISO/IEC 29151:2022	Clause 4.1; Clause 4.2; Annex A.2	Controller	Supporting	PII protection programme and policy
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Organizational privacy risk integration

1. Scope

1.1 This policy establishes the organization's Privacy Information Management System for the processing of PII in controller, joint controller, processor, and subprocessor contexts.

1.2 This policy applies to:

1.2.1 PIMS scope, context, interested parties, and organizational boundaries;

1.2.2 PIMS role determination for PII processing activities;

1.2.3 privacy policy, privacy objectives, privacy risk assessment, privacy risk treatment, and the PIMS Statement of Applicability;

1.2.4 PIMS governance, monitoring, internal audit, management review, nonconformity, corrective action, and continual improvement;

1.2.5 documented information and evidence needed to demonstrate PIMS conformity and accountability.

1.3 For this policy, a material change means any change that affects PIMS scope, PII processing purposes, PII categories, PII principal categories, processing locations, controller or processor role allocation, system architecture, supplier or subprocessor arrangements, privacy risk profile, applicable legal or contractual obligations, or certification scope.

2. Purpose

2.1 This policy defines the mandatory governance requirements for establishing, implementing, maintaining, monitoring, and continually improving the PIMS.

2.2 The purpose of this policy is to ensure that the organization can demonstrate accountable, risk-based, and evidence-driven management of PII processing across applicable PIMS roles.

3. Objectives

3.1 The objectives of this policy are to:

3.1.1 define the PIMS scope, context, boundaries, and role applicability;

3.1.2 assign governance accountability for the PIMS using canonical PIMS roles;

3.1.3 establish privacy objectives and measurable PIMS performance expectations;

3.1.4 maintain a PIMS Statement of Applicability for selected and excluded controls;

3.1.5 integrate privacy risk assessment, privacy risk treatment, and DPIA governance into PIMS operation;

3.1.6 ensure that controller, joint controller, processor, and subprocessor obligations are identified before processing begins;

3.1.7 maintain audit-ready evidence for certification readiness and continual improvement;

3.1.8 avoid unnecessary roles, registers, forms, and duplicate operational controls.

4. Policy Statements

4.1 PIMS establishment, context, and scope

4.1.1 [Both] Top Management MUST approve the PIMS scope in REG01 before initial PIMS implementation and within 30 days of any material change.

4.1.2 [Both] The Privacy Lead / PIMS Manager MUST document external and internal privacy context issues in REG01 annually and within 30 days of any material change.

4.1.3 [Both] The Privacy Lead / PIMS Manager MUST document relevant interested parties and their PIMS requirements in REG01 annually and within 30 days of any material change.

4.1.4 [Both] The Privacy Lead / PIMS Manager MUST maintain the PIMS process interaction summary in REG01 before each management review.

4.2 PIMS role determination

4.2.1 [Both] The Process Owner / Business Owner MUST classify the organization's PIMS role for each PII processing activity in REG02 before the processing activity begins.

4.2.2 [Joint Controller] The Vendor / Procurement Owner MUST document joint controller responsibility allocation in REG08 before joint processing begins.

4.2.3 [Processor] The Vendor / Procurement Owner MUST document customer processing instructions for processor activities in REG08 before service onboarding.

4.2.4 [Subprocessor] The Vendor / Procurement Owner MUST document upstream customer instructions and approved subprocessing arrangements in REG08 before subprocessing begins.

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

9. Exceptions

9.1 Exception request and approval

9.1.1 [All] The Process Owner / Business Owner MUST document any requested exception to this policy in REG12 before the deviation occurs.

9.1.2 [Both] The Privacy Lead / PIMS Manager MUST assess the privacy risk of each requested exception in REG04 before approval.

9.1.3 [Both] Top Management MUST approve exceptions that exceed accepted privacy risk thresholds in REG12 before implementation.

9.1.4 [Both] The Privacy Lead / PIMS Manager MUST review active PIMS exceptions in REG12 quarterly until closure.

9.2 Exception closure

9.2.1 [All] The Process Owner / Business Owner MUST document exception closure evidence in REG12 by the approved exception expiry date.

9.2.2 [Both] The Internal Audit / Compliance Reviewer MUST verify expired exception closure evidence in REG12 during the next planned internal audit.

10. Enforcement

10.1 Nonconformity handling

10.1.1 [All] The Privacy Lead / PIMS Manager MUST record suspected nonconformities with this policy in REG12 within five business days of identification.

10.1.2 [All] The Process Owner / Business Owner MUST implement approved corrective actions in REG12 by the assigned due date after nonconformity approval.

10.1.3 [All] Top Management MUST review unresolved major PIMS nonconformities in REG12 at each management review.

10.1.4 [All] The Internal Audit / Compliance Reviewer MUST verify corrective action effectiveness in REG12 within 30 days of reported closure.

10.2 Escalation

10.2.1 [All] The Privacy Lead / PIMS Manager MUST escalate overdue major corrective actions to Top Management in REG12 within five business days after the due date.

10.2.2 [All] Top Management MUST record decisions on overdue major corrective actions in REG12 within 15 business days of escalation.

11. Review and Maintenance

11.1 Policy review

11.1.1 [All] The Privacy Lead / PIMS Manager MUST review this policy in REG12 annually and within 30 days of any material legal, organizational, processing, technology, or certification scope change.

11.1.2 [All] The Data Protection Officer / Privacy Advisor MUST provide documented advice in REG12 before policy approval when material privacy obligations change.

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

11.1.4 [All] The Privacy Lead / PIMS Manager MUST update REG01 and REG03 within 15 business days after approved policy changes that alter PIMS scope or control applicability.

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

12. Related Policies

12.1 This policy is supported by the following related policies:

12.2 PII02 - Privacy Roles, Responsibilities and Accountability Policy

12.3 PII03 - PII Processing Inventory and Lawful Basis Policy

12.4 PII07 - Privacy Risk Assessment and DPIA Policy

12.5 PII08 - Privacy by Design and Default Policy

12.6 PII12 - Processor, Subprocessor and Data Sharing Policy

12.7 PII14 - PII Security and Access Control Policy

12.8 PII15 - PII Incident and Breach Management Policy

12.9 PII16 - Privacy Training, Awareness and Competence Policy

12.10 PII17 - PIMS Documented Information and Evidence Management Policy

12.11 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 4.1** - Mapped to determining organizational context, privacy context issues, and controller or processor role applicability for PIMS activities. Addressed by clauses [4.1.2; 4.2.1; 6.1.3].

13.2.2 **Clause 4.2** - Mapped to identifying interested parties, PII principals, customers, supervisory authorities, processors, subprocessors, and their relevant PIMS requirements. Addressed by clauses [4.1.3; 7.2.1; 11.1.1].

13.2.3 **Clause 4.3** - Mapped to defining, approving, maintaining, and changing the documented PIMS scope. Addressed by clauses [4.1.1; 6.1.3; 11.1.4].

13.2.4 **Clause 4.4** - Mapped to establishing, implementing, maintaining, and improving PIMS processes and their interactions. Addressed by clauses [4.1.4; 7.1.1; 7.2.1].

13.2.5 **Clause 5.1** - Mapped to Top Management approval, resources, governance review, and leadership over PIMS effectiveness and improvement. Addressed by clauses [4.3.1; 5.1.1; 6.1.1; 8.1.4; 10.1.3].

13.2.6 **Clause 5.2** - Mapped to maintaining this privacy policy as approved documented information and communicating policy changes. Addressed by clauses [4.3.1; 11.1.1; 11.1.3; 11.1.5].

13.2.7 **Clause 5.3** - Mapped to assigning and communicating PIMS roles, responsibilities, and authorities. Addressed by clauses [5.1.1; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.8 **Clause 6.1.1** - Mapped to planning actions for PIMS risks and opportunities using context, interested party requirements, objectives, and improvement inputs. Addressed by clauses [4.1.2; 4.1.3; 4.4.1; 6.1.1; 8.1.1].

13.2.9 **Clause 6.1.2** - Mapped to requiring privacy risk assessment before new or materially changed processing and maintaining privacy risk evidence. Addressed by clauses [4.4.1; 5.1.3; 8.2.4; 9.1.2].

13.2.10 **Clause 6.1.3** - Mapped to privacy risk treatment, control selection, information security programme linkage, and Statement of Applicability maintenance. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.3; 7.1.4; 8.2.2].

13.2.11 **Clause 6.2** - Mapped to establishing, measuring, monitoring, communicating, and updating PIMS objectives. Addressed by clauses [4.3.1; 4.3.2; 8.1.2; 8.1.4].

13.2.12 **Clause 6.3** - Mapped to planned PIMS changes and control of changes affecting scope, roles, controls, and documented information. Addressed by clauses [4.1.1; 6.1.3; 7.1.1; 11.1.4].

13.2.13 **Clause 7.1** - Mapped to determining and providing resources for PIMS establishment, operation, maintenance, and improvement. Addressed by clauses [5.1.1; 6.1.1; 7.1.1].

13.2.14 **Clause 7.2** - Mapped to competence expectations and evidence supporting PIMS responsibilities and role performance. Addressed by clauses [5.1.3; 5.1.8; 11.1.5].

13.2.15 **Clause 7.3** - Mapped to awareness of the privacy policy, contribution to PIMS effectiveness, and implications of nonconformity. Addressed by clauses [11.1.5; 10.1.1; 10.2.1].

13.2.16 **Clause 7.4** - Mapped to internal and external communications relevant to PIMS governance, policy changes, and escalation. Addressed by clauses [6.2.1; 10.2.1; 11.1.5].

13.2.17 **Clause 7.5** - Mapped to documented information creation, maintenance, control, evidence readiness, and retention. Addressed by clauses [4.5.1; 4.5.3; 7.1.6; 11.1.4].

13.2.18 **Clause 8.1** - Mapped to planning, implementing, and controlling PIMS operational processes and externally provided processes. Addressed by clauses [4.4.4; 7.1.3; 7.1.5; 7.2.1].

13.2.19 **Clause 8.2** - Mapped to performing privacy risk assessments at planned intervals and when significant changes are proposed or occur. Addressed by clauses [4.4.1; 8.2.4; 9.1.2].

13.2.20 **Clause 8.3** - Mapped to implementing privacy risk treatment plans and retaining evidence of treatment results. Addressed by clauses [4.4.3; 7.1.3; 8.2.2].

13.2.21 **Clause 9.1** - Mapped to monitoring, measurement, analysis, evaluation, metrics, and PIMS effectiveness reporting. Addressed by clauses [8.1.1; 8.1.2; 8.1.4; 8.2.1; 8.2.2; 8.2.3; 8.2.4].

13.2.22 **Clause 9.2** - Mapped to internal audit planning, evidence sampling, audit results, and independent review. Addressed by clauses [5.1.9; 6.2.1; 8.1.3; 9.2.2].

13.2.23 **Clause 9.3** - Mapped to management review inputs, performance review, management review outputs, and improvement decisions. Addressed by clauses [6.1.1; 6.1.2; 8.1.4; 10.1.3].

13.2.24 **Clause 10.1** - Mapped to continual improvement through management review, metrics, corrective action tracking, and policy maintenance. Addressed by clauses [6.1.1; 6.2.2; 10.1.4; 11.1.1].

13.2.25 **Clause 10.2** - Mapped to nonconformity handling, corrective action, escalation, closure, and effectiveness verification. Addressed by clauses [4.5.2; 6.2.2; 6.2.3; 10.1.1; 10.1.2; 10.1.4; 10.2.1; 10.2.2].

13.2.26 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9** - Mapped to controller-side processing purpose records, lawful basis linkage, DPIA need determination,

joint controller responsibility allocation, and processing evidence records. Addressed by clauses [4.2.1; 4.2.2; 4.4.2; 4.5.1; 7.1.2; 8.2.1].

13.2.27 **Annex A.2.2.2; Annex A.2.2.3** - Mapped to processor customer agreements, documented customer instructions, and processor purpose limitations. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.2.28 **Annex A.3.3** - Mapped to PII security policy linkage, PII security control baseline ownership, and information security control status in the PIMS Statement of Applicability. Addressed by clauses [4.3.4; 5.1.4; 7.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapped to accountability evidence, policy approval, processing role classification, control applicability, monitoring, audit, and corrective action records. Addressed by clauses [4.3.1; 4.5.1; 4.5.2; 6.1.1; 8.1.3].

13.3.2 **Article 24** - Mapped to controller governance measures, policy approval, PIMS objectives, review of effectiveness, and documented evidence of controller accountability. Addressed by clauses [4.3.1; 4.3.2; 6.1.1; 8.1.4; 11.1.1].

13.3.3 **Article 26** - Mapped to determining and documenting joint controller responsibility allocation before joint processing begins. Addressed by clauses [4.2.2; 5.1.7; 7.1.5].

13.3.4 **Article 28** - Mapped to processor and subprocessor governance records, customer processing instructions, and externally provided process control. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.3.5 **Article 30** - Mapped to processing activity records, role classification, processing accountability records, and evidence retained for auditability. Addressed by clauses [4.2.1; 5.1.5; 7.1.2; 8.2.1].

13.3.6 **Article 32** - Mapped to PII security baseline governance, security control ownership, security implementation status, and operational control confirmation. Addressed by clauses [4.3.4; 4.4.4; 5.1.4; 7.1.4].

13.3.7 **Article 35** - Mapped to DPIA need determination and privacy risk assessment before high-risk or materially changed controller processing proceeds. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12** - Mapped to privacy control identification, privacy principles, information security, privacy compliance, audit, evidence, and risk-based privacy governance. Addressed by clauses [4.3.3; 4.3.4; 4.4.1; 4.5.1; 8.1.3; 10.1.4].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Mapped to PIA governance, DPIA trigger determination, PIA preparation, privacy risk criteria, and documented privacy risk assessment evidence. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4; 9.1.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2; Annex A.2** - Mapped to PII protection programme requirements, PII protection requirement identification, privacy risk-based control selection, and PII protection policy direction. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.4].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - Mapped to organizational privacy risk principles, leadership commitment, integration of privacy risk into PIMS governance, and understanding the organization’s role in PII processing. Addressed by clauses [4.1.2; 4.2.1; 4.4.1; 4.4.3; 6.1.1].