					Insert Registered Legal Entity Name Here							
Document number: PII02					Document Title: **Privacy Roles, Responsibilities and Accountability 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	PIMS role context
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Leadership and accountability
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	PIMS roles, responsibilities and authorities
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Role competence
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Role awareness
ISO/IEC 27701:2025	Clause 7.4	Both	Supporting	Role communication
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Role documented information
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Operational control ownership
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Independent audit role
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Management review of accountability
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Role-related nonconformity and corrective action
ISO/IEC 27701:2025	Annex A.1.2.7	Controller	Supporting	Processor contract responsibility
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Primary	Joint controller roles and responsibilities
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Accountability records
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Processor customer agreements and instructions
ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Supporting	Processor purpose alignment
GDPR	Article 5(2)	Controller	Supporting	Accountability evidence

GDPR	Article 24	Controller	Supporting	Controller responsibility and measures
GDPR	Article 26	Joint Controller	Supporting	Joint controller arrangements
GDPR	Article 28	Both	Supporting	Processor governance and instructions
GDPR	Article 30	Both	Supporting	Processing records and responsibility evidence
GDPR	Article 37	Conditional	Referenced	DPO designation where applicable
GDPR	Article 38	Conditional	Supporting	DPO position and independence where applicable
GDPR	Article 39	Conditional	Supporting	DPO tasks where applicable
ISO/IEC 29100:2020	Clause 4.1; Clause 4.2	Both	Supporting	Privacy framework actors and roles
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Privacy compliance accountability
ISO/IEC 29151:2022	Clause 6.1.2; Clause 6.1.3	Both	Supporting	PII protection roles and segregation
ISO/IEC 27002:2022	Control 5.2	Both	Supporting	Information security roles and responsibilities
ISO/IEC 27002:2022	Control 5.3	Both	Supporting	Segregation of duties

1. Scope

1.1 This policy defines the PIMS role model, accountability structure, responsibility assignment rules, role-combination rules, escalation expectations, and evidence requirements for privacy governance.

1.2 This policy applies to personnel, functions, systems, suppliers, processors, subprocessors, and joint controller relationships that participate in or influence PII processing within the PIMS scope.

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

1.4 This policy does not create new organizational job titles. It defines canonical PIMS roles that may be assigned to existing personnel or functions, provided that role assignment, competence, independence, and conflict-of-interest requirements are documented.

2. Purpose

2.1 The purpose of this policy is to ensure that PIMS responsibilities are clearly assigned, understood, communicated, evidenced, reviewed, and improved.

2.2 This policy enables the organization to demonstrate accountability for privacy governance, PII processing ownership, controller and processor role determination, joint controller responsibility allocation, processor instruction handling, supplier privacy responsibility, independent review, and role-based escalation.

3. Objectives

3.1 The objectives of this policy are to:

3.1.1 define the canonical PIMS roles used across the PIMS policy set;

3.1.2 ensure that every material PIMS responsibility has an assigned accountable role;

3.1.3 support controller, joint controller, processor, and subprocessor accountability;

3.1.4 permit practical role combination for small and medium-sized organizations while controlling conflicts of interest;

3.1.5 preserve independent review by the Internal Audit / Compliance Reviewer;

3.1.6 ensure that role assignments and role changes are recorded in canonical evidence objects;

3.1.7 ensure that PIMS role holders receive appropriate communication and awareness;

3.1.8 ensure that role-related gaps, conflicts, and nonconformities are escalated and corrected.

4. Policy Statements

4.1 PIMS role model and assignment

4.1.1 [All] Top Management MUST approve the canonical PIMS role model in REG01 before initial PIMS implementation and annually thereafter.

4.1.2 [All] The Privacy Lead / PIMS Manager MUST maintain named PIMS role assignments in REG01 before PIMS implementation and within 10 business days of personnel or organizational changes.

4.1.3 [All] The Privacy Lead / PIMS Manager MUST document the responsibility scope and authority level for each assigned PIMS role in REG01 before the assignment takes effect.

4.1.4 [All] The Process Owner / Business Owner MUST assign an accountable processing owner for each PII processing activity in REG02 before the processing activity begins.

4.1.5 [All] The System Owner / Application Owner MUST document the accountable system owner for each PII-processing system in REG02 before system go-live.

4.1.6 [All] The Vendor / Procurement Owner MUST document the relationship owner for each processor, subprocessor, third-party data sharing, or joint controller relationship in REG08 before onboarding or agreement approval.

4.2 Role combination, segregation, and independence

4.2.1 [All] The Privacy Lead / PIMS Manager MUST document each PIMS role combination in REG01 before the role combination takes effect.

4.2.2 [All] Top Management MUST approve role combinations involving the Privacy Lead / PIMS Manager, Data Protection Officer / Privacy Advisor, Information Security Lead, Incident Response Coordinator, or Internal Audit / Compliance Reviewer in REG01 before assignment.

4.2.3 [All] The Internal Audit / Compliance Reviewer MUST document independence from the PIMS process being reviewed in REG12 before each PIMS audit or compliance review starts.

4.2.4 [All] The Privacy Lead / PIMS Manager MUST record compensating controls for unavoidable segregation conflicts in REG12 before approving a role combination.

4.2.5 [All] The Data Protection Officer / Privacy Advisor MUST record role independence concerns or conflict-of-interest concerns in REG12 within five business days of identification.

[... 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 a role-accountability exception in REG12 before operating a PII processing activity without a required assigned role.

9.1.2 [All] The Privacy Lead / PIMS Manager MUST assess the impact and mitigation of each role-accountability exception in REG12 within 10 business days of request.

9.1.3 [All] Top Management MUST approve role-accountability exceptions exceeding 30 days or affecting high-risk processing in REG12 before the exception takes effect.

9.1.4 [All] The Privacy Lead / PIMS Manager MUST set an expiry date not exceeding 90 days in REG12 for each approved role-accountability exception before approval.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST close or reassess each role-accountability exception in REG12 within five business days of expiry.

10. Enforcement

10.1.1 [All] The Privacy Lead / PIMS Manager MUST record missing, inaccurate, or outdated PIMS role assignments as nonconformities in REG12 within five business days of identification.

10.1.2 [All] Top Management MUST require corrective action in REG12 within 15 business days for repeated or prolonged accountability failures.

10.1.3 [All] The Process Owner / Business Owner MUST prevent go-live of new or changed PII processing where required role and accountability evidence is absent from REG02 or REG08.

10.1.4 [All] The Internal Audit / Compliance Reviewer MUST verify corrective action effectiveness for role-accountability 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 the PIMS role model.

11.1.2 [All] The Data Protection Officer / Privacy Advisor MUST review proposed changes to this policy for privacy role impact in REG12 before approval.

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 REG11 within 15 business days after approved changes to PIMS roles, responsibilities, or communication requirements.

12. Related Policies

12.1 This policy is supported by the following related policies:

12.2 PII01 - Privacy Information Management System 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 Third-Party Privacy Management 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 PIMS role context, controller and processor applicability, processing ownership, and relationship responsibility records. Addressed by clauses [4.3.5; 5.1.5; 5.1.7; 7.1.2].

13.2.2 **Clause 5.1** - Mapped to Top Management approval, accountability oversight, annual management review, accountability metrics, and corrective action for role failures. Addressed by clauses [4.1.1; 4.2.2; 5.1.1; 6.1.1; 8.1.6; 10.1.2; 11.1.3].

13.2.3 **Clause 5.3** - Mapped to assignment, documentation, communication, and maintenance of PIMS roles, responsibilities, authorities, system ownership, processing ownership, supplier relationship ownership, incident escalation ownership, and independent review responsibility. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.4.2; 4.4.3; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.4 **Clause 7.2** - Mapped to role-specific competence and awareness evidence for assigned PIMS responsibilities. Addressed by clauses [7.1.4; 8.1.5].

13.2.5 **Clause 7.3** - Mapped to awareness of assigned PIMS responsibilities, acknowledgement evidence, and annual role awareness reporting. Addressed by clauses [4.5.1; 4.5.2; 7.1.4; 8.1.5].

13.2.6 **Clause 7.4** - Mapped to communication of role assignments, role changes, escalations, and role handover information. Addressed by clauses [4.5.1; 4.5.4; 6.1.5; 7.1.6].

13.2.7 **Clause 7.5** - Mapped to documented information for PIMS role assignments, responsibility scopes, authority levels, annual evidence retention, and role matrix maintenance. Addressed by clauses [4.1.2; 4.1.3; 4.5.3; 7.1.1; 11.1.4].

13.2.8 **Clause 8.1** - Mapped to operational control ownership for processing activities, systems, suppliers, processors, subprocessors, joint controller relationships, and go-live controls. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 7.1.2; 7.1.3; 7.1.5; 10.1.3].

13.2.9 **Clause 9.2** - Mapped to independent audit and compliance review of role assignment evidence, role-combination evidence, independence evidence, findings, and corrective action closure. Addressed by clauses [4.2.3; 5.1.9; 6.1.4; 8.1.4; 10.1.4].

13.2.10 **Clause 9.3** - Mapped to management review of PIMS role assignment completeness, role conflicts, exceptions, accountability metrics, and accountability review outputs. Addressed by clauses [5.1.1; 6.1.1; 8.1.6; 11.1.1].

13.2.11 **Clause 10.2** - Mapped to escalation, nonconformity recording, corrective action, exception closure, and effectiveness verification for role-accountability issues. Addressed by clauses [4.2.5; 4.4.5; 6.1.5; 9.1.5; 10.1.1; 10.1.2; 10.1.4].

13.2.12 **Annex A.1.2.7** - Mapped to assigning and documenting processor contract responsibility and third-party responsibility escalation before contract approval or renewal. Addressed by clauses [4.1.6; 4.4.4; 5.1.7; 7.1.3].

13.2.13 **Annex A.1.2.8** - Mapped to documenting joint controller responsibility allocation and relationship responsibility evidence before joint controller processing begins. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.2.14 **Annex A.1.2.9** - Mapped to maintaining accountability records for controller processing ownership, role classification, and evidence ownership. Addressed by clauses [4.3.1; 4.3.5; 4.5.3; 8.1.1].

13.2.15 **Annex A.2.2.2** - Mapped to processor customer agreement responsibility, customer instruction ownership, and processor relationship evidence. Addressed by clauses [4.3.3; 5.1.7; 7.1.3; 8.1.3].

13.2.16 **Annex A.2.2.3** - Mapped to processor purpose and instruction alignment through customer instruction ownership and controller/processor role verification. Addressed by clauses [4.3.3; 4.3.5; 5.1.7].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapped to accountability evidence for role assignments, processing ownership, role reviews, nonconformities, and audit findings. Addressed by clauses [4.5.3; 6.1.2; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Mapped to controller responsibility, accountable processing ownership, Top Management oversight, annual review, and accountability measures. Addressed by clauses [4.1.1; 4.3.1; 5.1.1; 6.1.1; 8.1.6].

13.3.3 **Article 26** - Mapped to documenting joint controller responsibility allocation and relationship responsibility evidence before joint controller processing begins. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.3.4 **Article 28** - Mapped to processor and subprocessor responsibility allocation, customer instruction ownership, contract responsibility, and third-party escalation paths. Addressed by clauses [4.3.3; 4.3.4; 4.4.4; 5.1.7; 7.1.3].

13.3.5 **Article 30** - Mapped to processing records, processing ownership, PIMS role classification, and controller/processor role verification. Addressed by clauses [4.1.4; 4.3.1; 4.3.5; 8.1.1].

13.3.6 **Article 37** - Mapped to documenting the Data Protection Officer / Privacy Advisor role where designation is applicable or voluntarily assigned. Addressed by clauses [4.1.2; 4.1.3; 5.1.3; 11.1.2].

13.3.7 **Article 38** - Mapped to the position, independence, involvement, and conflict-of-interest handling of the Data Protection Officer / Privacy Advisor where applicable. Addressed by clauses [4.2.5; 5.1.3; 6.1.3; 11.1.2].

13.3.8 **Article 39** - Mapped to privacy advice, monitoring observations, advisory review, and role-related privacy impact review by the Data Protection Officer / Privacy Advisor where applicable. Addressed by clauses [4.4.1; 5.1.3; 6.1.3; 11.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.1; Clause 4.2** - Mapped to privacy framework actors and role allocation for PII principals, PII controllers, PII processors, third parties, and PIMS role classification. Addressed by clauses [4.1.4; 4.1.6; 4.3.5; 5.1.5; 5.1.7].

13.4.2 **Clause 5.12** - Mapped to privacy compliance accountability, role evidence, review, audit findings, and corrective action verification. Addressed by clauses [4.5.3; 6.1.2; 8.1.4; 10.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 6.1.2; Clause 6.1.3** - Mapped to PII protection role definition, role documentation, role communication, security/privacy coordination, and segregation of duties for PII protection. Addressed by clauses [4.1.1; 4.2.1; 4.2.3; 4.2.4; 4.4.2; 5.1.4; 7.1.4].

13.6 ISO/IEC 27002:2022

13.6.1 Control 5.2 - Mapped to defining, allocating, documenting, communicating, and maintaining PIMS and information security responsibilities. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.2; 4.5.1; 5.1.4; 7.1.1].

13.6.2 Control 5.3 - Mapped to segregation of duties, role-combination approval, independent review, conflict controls, and corrective action verification for role conflicts. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 9.1.2; 10.1.4].