					Insert Registered Legal Entity Name Here							
Document number: PII18					Document Title: **PIMS Monitoring, Audit and Improvement 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 6.2	Both	Supporting	Privacy objectives measurement
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Monitoring, audit and improvement documented information
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Operational planning and control monitoring
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Monitoring, measurement, analysis 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.1.2.9	Controller	Supporting	Controller processing records used for audit
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Processor agreement and audit cooperation evidence
GDPR	Article 5(2)	Controller	Supporting	Accountability evidence
GDPR	Article 24	Controller	Supporting	Controller measures and effectiveness review
GDPR	Article 28	Both	Supporting	Processor audit and cooperation governance
GDPR	Article 30	Both	Supporting	Processing records used for audit

GDPR	Article 32	Both	Supporting	Testing and evaluating security measures
GDPR	Article 39	Conditional	Supporting	DPO monitoring and audit advice where applicable
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Privacy compliance, audit and independent supervision
ISO/IEC 29151:2022	Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	PII protection review and compliance checks
ISO/IEC 27001:2022	Clause 9.1	Both	Supporting	Information security monitoring and evaluation
ISO/IEC 27001:2022	Clause 9.2	Both	Supporting	ISMS internal audit support
ISO/IEC 27001:2022	Clause 9.3	Both	Supporting	ISMS management review support
ISO/IEC 27001:2022	Clause 10.1	Both	Supporting	ISMS continual improvement support
ISO/IEC 27001:2022	Clause 10.2	Both	Supporting	ISMS nonconformity and corrective action support
ISO/IEC 27002:2022	Control 5.35	Both	Supporting	Independent review of information security
ISO/IEC 27002:2022	Control 5.36	Both	Supporting	Compliance review of policies and standards
ISO 19011:2018	Clause 4; Clause 5; Clause 6; Clause 7	Both	Supporting	Management-system audit principles, programme, conduct and competence

1. Scope

1.1 This policy defines the organization's requirements for PIMS monitoring, measurement, analysis, evaluation, internal audit, management review, nonconformity handling, corrective action, and continual improvement.

1.2 This policy applies to:

1.2.1 all PIMS processes, controls, policies, registers, evidence objects, systems, suppliers, processors, subprocessors, and data sharing arrangements within the PIMS scope;

1.2.2 the organization's controller, joint controller, processor, and subprocessor contexts;

1.2.3 the consolidated monitoring of PIMS performance, privacy objectives, control implementation status, audit findings, nonconformities, corrective actions, management review actions, and improvement actions;

1.2.4 evidence retained in REG12 and supporting source evidence retained in REG01 through REG11.

1.3 This policy does not replace operational monitoring requirements defined in other PIMS policies. It establishes the consolidated performance evaluation, audit, review, and improvement cycle for the PIMS.

1.4 For this policy, a major PIMS nonconformity means a failure that materially affects PIMS scope, privacy objectives, PII processing accountability, privacy risk treatment, PII principal rights, security of processing, processor or subprocessor governance, breach readiness, documented evidence integrity, certification scope, or repeated failure of the same requirement within a 12-month period.

1.5 For this policy, a material change means any change affecting 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, audit scope, monitoring method, or certification scope.

2. Purpose

2.1 The purpose of this policy is to ensure that the organization evaluates PIMS performance, verifies PIMS conformity, identifies nonconformities, corrects control weaknesses, and continually improves the PIMS using objective evidence.

2.2 This policy enables the organization to demonstrate that PIMS monitoring, audit, management review, and improvement activities are planned, independent where required, evidence-based, timely, and traceable to accountable roles and canonical evidence objects.

3. Objectives

3.1 The objectives of this policy are to:

3.1.1 define a consolidated PIMS monitoring and measurement process;

3.1.2 ensure privacy objectives and PIMS control performance are measured using documented evidence;

3.1.3 establish a risk-based internal audit programme for the PIMS;

3.1.4 preserve independence and objectivity in PIMS audit activities;

3.1.5 ensure management review receives complete and current PIMS performance inputs;

3.1.6 ensure nonconformities are recorded, assessed, corrected, and verified;

3.1.7 ensure corrective actions are tracked to closure and reviewed for effectiveness;

3.1.8 identify recurring weaknesses and improvement opportunities;

3.1.9 support certification readiness and accountable evidence management;

3.1.10 avoid duplicating operational metrics already defined in related PIMS policies.

4. Policy Statements

4.1 PIMS monitoring and measurement framework

4.1.1 [Both] The Privacy Lead / PIMS Manager MUST define the consolidated PIMS monitoring programme in REG12 before initial PIMS operation and annually thereafter.

4.1.2 [Both] The Privacy Lead / PIMS Manager MUST define the measurement method, frequency, evidence source, target, and responsible role for each PIMS metric in REG12 before the measurement cycle begins.

4.1.3 [Both] The Process Owner / Business Owner MUST provide PII processing activity monitoring inputs from REG02 to the Privacy Lead / PIMS Manager quarterly.

4.1.4 [Both] The Information Security Lead MUST provide PII security control status inputs from REG03 to the Privacy Lead / PIMS Manager quarterly.

4.1.5 [Both] The Vendor / Procurement Owner MUST provide processor, subprocessor, third-party sharing, and supplier assurance status inputs from REG08 to the Privacy Lead / PIMS Manager quarterly.

4.1.6 [All] The Incident Response Coordinator MUST provide privacy incident and breach trend inputs from REG10 to the Privacy Lead / PIMS Manager monthly and within 10 business days after major incident closure.

4.1.7 [Both] The Privacy Lead / PIMS Manager MUST consolidate PIMS monitoring results in REG12 quarterly.

4.2 PIMS internal audit programme

4.2.1 [All] The Internal Audit / Compliance Reviewer MUST prepare a risk-based PIMS internal audit programme in REG12 annually before the first planned PIMS audit cycle.

4.2.2 [All] The Internal Audit / Compliance Reviewer MUST define the objective, criteria, scope, method, sample basis, and reporting deadline for each PIMS audit in REG12 before audit fieldwork begins.

4.2.3 [All] The Internal Audit / Compliance Reviewer MUST record auditor independence and conflict-of-interest checks in REG12 before each audit assignment.

4.2.4 [All] The Privacy Lead / PIMS Manager MUST make requested controlled PIMS documented information and register evidence available through REG12 within 10 business days of an approved audit request.

4.2.5 [Both] The Internal Audit / Compliance Reviewer MUST test applicable PIMS control implementation status against REG03 during each PIMS audit.

4.2.6 [Both] The Internal Audit / Compliance Reviewer MUST record the selected PII processing evidence sample in REG12 during each PIMS audit.

4.2.7 [All] The Internal Audit / Compliance Reviewer MUST record PIMS audit results in REG12 within 15 business days after audit completion.

4.2.8 [All] The Privacy Lead / PIMS Manager MUST assign corrective action owners for accepted PIMS audit findings in REG12 within 10 business days of audit result acceptance.

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

9. Exceptions

9.1 Monitoring, audit and improvement exceptions

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

9.1.2 [All] The Privacy Lead / PIMS Manager MUST assess the privacy, certification, audit, and corrective action impact of each requested 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 affecting legal obligations, PII principal rights, DPIA commitments, customer audit obligations, or high-risk processing.

9.1.4 [All] Top Management MUST approve exceptions affecting audit schedule completion, management review, major nonconformities, certification scope, or high-risk processing 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 monitoring, audit, or improvement exception.

9.1.6 [All] The Privacy Lead / PIMS Manager MUST close or reassess each monitoring, audit, or improvement exception in REG12 within five business days of expiry.

10. Enforcement

10.1 Enforcement of monitoring, audit and improvement requirements

10.1.1 [All] The Privacy Lead / PIMS Manager MUST record a missed monitoring cycle, missed PIMS audit, overdue management review, missing audit evidence, overdue corrective action, or overdue improvement action as a nonconformity in REG12 within five business days of identification.

10.1.2 [All] The Internal Audit / Compliance Reviewer MUST record audit finding severity in REG12 before audit report issuance.

10.1.3 [All] Top Management MUST require corrective action for each major PIMS nonconformity in REG12 within 10 business days of escalation.

10.1.4 [All] The Process Owner / Business Owner MUST prevent go-live or external assurance submission for high-risk processing where required corrective action evidence is missing from REG12 before go-live or submission.

10.1.5 [All] The Privacy Lead / PIMS Manager MUST escalate repeated missed monitoring or corrective action deadlines to Top Management in REG12 within five business days after the second occurrence in a 12-month period.

10.1.6 [All] The Internal Audit / Compliance Reviewer MUST verify enforcement action closure in REG12 at the next scheduled audit or within 60 days of reported closure, whichever occurs first.

11. Review and Maintenance

11.1 Policy review and maintenance

11.1.1 [All] The Privacy Lead / PIMS Manager MUST review this policy in REG12 annually and within 30 days of material change to PIMS monitoring, audit, management review, corrective action, or certification requirements.

11.1.2 [All] The Internal Audit / Compliance Reviewer MUST review PIMS audit programme effectiveness in REG12 annually after the final scheduled audit for the PIMS operating year.

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 update REG01 and REG03 within 15 business days after approved changes to this policy that alter PIMS scope or control applicability.

11.1.6 [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 PII17 - PIMS Documented Information and Evidence Management 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 6.2** - Mapped to defining, measuring, reporting, and reviewing PIMS objectives and PIMS performance metrics. Addressed by clauses [4.1.2; 4.3.4; 8.1.1].

13.2.2 **Clause 7.5** - Mapped to maintaining documented information for monitoring results, audit programmes, audit results, management review evidence, nonconformities, corrective actions, and improvement actions. Addressed by clauses [4.1.7; 4.2.4; 4.2.7; 4.3.1; 4.4.1; 7.1.8; 11.1.1].

13.2.3 **Clause 8.1** - Mapped to operating the planned PIMS monitoring, audit, corrective action, and improvement cycle as part of PIMS operational control. Addressed by clauses [4.1.1; 4.2.1; 7.1.1; 7.1.6].

13.2.4 **Clause 9.1** - Mapped to defining what is monitored and measured, consolidating monitoring results, evaluating PIMS performance, and maintaining measurement evidence. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.1.7; 8.1.1; 8.1.2; 8.1.4; 8.1.7].

13.2.5 **Clause 9.2** - Mapped to maintaining the internal audit programme, audit planning, auditor independence checks, evidence sampling, audit results, and audit finding follow-up. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 8.1.3; 10.1.2].

13.2.6 **Clause 9.3** - Mapped to management review planning, review of PIMS performance, review of audit and corrective action trends, approval of outputs, and resource decisions. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 6.1.7].

13.2.7 **Clause 10.1** - Mapped to identifying, approving, implementing, and tracking continual improvement opportunities for PIMS suitability, adequacy, and effectiveness. Addressed by clauses [4.3.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 7.1.6].

13.2.8 **Clause 10.2** - Mapped to recording nonconformities, root cause analysis, corrective action planning, corrective action implementation, effectiveness verification, escalation, and enforcement. Addressed by clauses [4.2.8; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 10.1.1; 10.1.3; 10.1.6].

13.2.9 **Annex A.1.2.9** - Mapped to controller processing records used as evidence sources for monitoring, audit sampling, and processing inventory currency metrics. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.2.10 **Annex A.2.2.2** - Mapped to processor agreement, customer audit, assurance response, and processor cooperation evidence tracked through supplier and customer assurance processes. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapped to accountability evidence for monitoring, audit, management review, corrective action, and continual improvement. Addressed by clauses [4.1.7; 4.2.7; 4.3.2; 4.4.2; 4.5.1].

13.3.2 **Article 24** - Mapped to controller governance measures, review of effectiveness, management review, corrective action, and documented improvement evidence. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.5.2; 10.1.3].

13.3.3 **Article 28** - Mapped to processor, subprocessor, customer audit, third-party assurance, and supplier cooperation evidence. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3.4 **Article 30** - Mapped to processing records used as monitoring, audit sampling, evidence-object completeness, and processing inventory currency evidence. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.3.5 **Article 32** - Mapped to monitoring and evaluating PII security control status, technical control evidence, and security-related effectiveness evidence. Addressed by clauses [4.1.4; 4.2.5; 5.1.4; 7.1.4; 8.1.2].

13.3.6 **Article 39** - Mapped to privacy advice, monitoring observations, audit support, and privacy compliance trend review by the Data Protection Officer / Privacy Advisor where applicable. Addressed by clauses [5.1.3; 6.1.6; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Mapped to privacy compliance verification, internal or independent audits, internal controls, supervision mechanisms, and privacy risk assessment evidence. Addressed by clauses [4.2.1; 4.2.3; 4.2.7; 4.5.1; 6.1.6; 8.1.7].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.2.2; Clause 18.2.3; Clause 18.2.4** - Mapped to independent review of PII-related information security, compliance with policies and standards, and technical compliance review for PII protection. Addressed by clauses [4.2.3; 4.2.5; 7.1.4; 8.1.2; 10.1.6].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 9.1** - Mapped to information security monitoring and evaluation inputs that support PIMS performance measurement and PII security control status. Addressed by clauses [4.1.4; 8.1.2].

13.6.2 **Clause 9.2** - Mapped to ISMS internal audit support for PIMS audit planning, audit evidence, audit results, and audit programme completion. Addressed by clauses [4.2.1; 4.2.2; 4.2.7; 8.1.3].

13.6.3 **Clause 9.3** - Mapped to management review inputs and outputs for integrated PIMS and information security performance oversight. Addressed by clauses [4.3.1; 4.3.2; 4.3.5; 4.3.6].

13.6.4 **Clause 10.1** - Mapped to continual improvement of the PIMS and supporting information security control environment. Addressed by clauses [4.5.1; 4.5.2; 4.5.6].

13.6.5 **Clause 10.2** - Mapped to nonconformity handling, corrective action planning, corrective action implementation, and effectiveness verification. Addressed by clauses [4.4.2; 4.4.4; 4.4.6; 4.4.7; 10.1.1].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.35 - Mapped to independent review, auditor independence checks, audit evidence testing, and independent verification of corrective action effectiveness. Addressed by clauses [4.2.3; 4.2.5; 4.4.7; 10.1.6].

13.7.2 Control 5.36 - Mapped to compliance review of PIMS and information security policies, control implementation status, and standards conformity evidence. Addressed by clauses [4.1.4; 4.2.5; 4.5.3; 8.1.2].

13.8 ISO 19011:2018

13.8.1 **Clause 4; Clause 5; Clause 6; Clause 7** - Mapped to audit principles, audit programme management, audit conduct, evidence-based audit reporting, audit follow-up, and auditor competence expectations for PIMS audits. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.6; 4.2.7; 4.4.7; 5.1.9; 11.1.2].