					Insert Registered Legal Entity Name Here							
Document number: PII15					Document Title: **PII Incident and Breach 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 7.4; Clause 7.5	Both	Supporting	PIMS communications and documented breach evidence
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Operational control, privacy risk assessment, and treatment linkage
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitoring, evaluation, nonconformity, corrective action, and improvement
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Incident management planning and preparation for PII processing
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Response to information security incidents involving PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Legal, statutory, regulatory, contractual requirements and protection of records
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Processor customer agreement and customer obligation support
GDPR	Article 5(2); Article 24	Controller	Supporting	Accountability and controller responsibility
GDPR	Article 26	Joint Controller	Supporting	Joint-controller breach responsibility coordination
GDPR	Article 28	Both	Supporting	Processor assistance and processor contract obligations

GDPR	Article 32	Both	Supporting	Security of processing and breach detection capability
GDPR	Article 33	Both	Primary	Personal data breach notification and breach documentation
GDPR	Article 34	Controller	Primary	Communication of personal data breaches to affected PII principals
GDPR	Article 39	Conditional	Supporting	DPO advice, monitoring, cooperation, and contact-point support
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Information security and privacy compliance principles
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	PII incident response responsibilities and event reporting
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Incident planning, assessment, response, lessons learned, and evidence collection
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Incident management process lifecycle
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Incident policy, plan, awareness, testing, and lessons learned
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Detection, notification, triage, analysis, response, and reporting operations
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Cloud processor notification and breach record expectations

NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Significant incident reporting where applicable
DORA Regulation (EU) 2022/2554	Article 17; Article 18; Article 19	Conditional	Supporting	ICT incident management, classification, and reporting where applicable

1. Scope

1.1 This policy defines the requirements for identifying, reporting, triaging, assessing, containing, notifying, documenting, closing, and improving from PII incidents and PII breaches within the PIMS scope.

1.2 This policy applies to the following PIMS roles, systems, applications, services, processes, suppliers, processors, subprocessors, and third parties:

1.2.1 the organization acting as a PII controller;

1.2.2 the organization acting as a joint controller where breach responsibility coordination is required;

1.2.3 the organization acting as a PII processor;

1.2.4 the organization acting as a subprocessor;

1.2.5 systems, applications, services, processes, suppliers, processors, subprocessors, and third parties that process, store, transmit, support, access, or otherwise affect PII within the PIMS scope.

1.3 This policy uses REG10 - PII Incident and Breach Register as the primary evidence object for PII incident and breach management.

1.4 This policy uses supporting evidence objects as follows:

1.4.1 REG01 for PIMS scope, applicable interested-party, legal, contractual, sectoral, and customer reporting context.

1.4.2 REG02 for affected processing activities, PII categories, PII principal categories, purposes, and systems.

1.4.3 REG03 for Statement of Applicability and control applicability updates.

1.4.4 REG04 for privacy risk, DPIA, and residual risk linkage.

1.4.5 REG08 for processor, subprocessor, customer, supplier, and third-party incident interface evidence.

1.4.6 REG09 for international transfer linkage when an incident affects cross-border processing.

1.4.7 REG11 for training, awareness, and incident-response competence evidence.

1.4.8 REG12 for audit, nonconformity, corrective action, and improvement evidence.

1.5 This policy relies on related PIMS policies for specialist controls:

1.5.1 PII03 governs processing inventory and lawful basis records.

1.5.2 PII04 governs privacy notice and transparency controls outside breach-specific communications.

1.5.3 PII06 governs PII principal rights requests that arise before, during, or after an incident.

1.5.4 PII07 governs privacy risk assessment and DPIA methodology.

1.5.5 PII08 governs privacy by design and default controls.

1.5.6 PII10 governs retention, deletion, and disposal controls.

1.5.7 PII12 governs processor, subprocessor, supplier, and third-party privacy relationship controls.

1.5.8 PII13 governs international PII transfer mechanisms and transfer risk records.

1.5.9 PII14 governs preventive and detective PII security and access controls.

1.5.10 PII16 governs privacy training, awareness, and competence.

1.5.11 PII17 governs documented information and evidence management.

1.5.12 PII18 governs monitoring, internal audit, management review, nonconformity, corrective action, and continual improvement.

1.6 For this policy, the following definitions apply:

1.6.1 "PII incident" means a suspected or confirmed event that has affected, may have affected, or could reasonably affect the confidentiality, integrity, availability, lawful processing, or authorized handling of PII.

1.6.2 "PII breach" means a confirmed PII incident involving unauthorized, unlawful, accidental, or unintended destruction, loss, alteration, disclosure of, access to, unavailability of, or compromise of PII.

1.6.3 "Breach assessment" means the documented evaluation of whether a PII incident is a PII breach, what PII and PII principals are affected, what risks may arise, what notifications or communications are required, and what remedial action is needed.

1.6.4 "Awareness" means the point at which the organization has a reasonable degree of certainty that a security or privacy incident has occurred and PII has been or may have been compromised.

1.6.5 "High-impact PII incident" means a PII incident involving high-risk processing, special category or highly sensitive PII, large-scale PII, vulnerable individuals, regulated customers, multi-jurisdictional impact, material customer impact, privileged access compromise, public exposure, ransomware, service unavailability, or significant operational or reputational impact.

1.6.6 "Material incident change" means new or changed information affecting incident scope, severity, PII categories, PII principal impact, notification decision, customer impact, root cause, containment, recovery, corrective action, or external reporting obligations.

2. Purpose

2.1 The purpose of this policy is to ensure that PII incidents and breaches are handled consistently, promptly, lawfully, securely, and with audit-ready evidence.

2.2 This policy supports accountability by requiring PII incidents and breaches to be recorded in REG10, linked to affected processing records, privacy risks, processor and subprocessor relationships, transfer records, corrective actions, and training records where triggered.

2.3 This policy ensures that controller, joint controller, processor, and subprocessor obligations are handled through distinct applicability rules while maintaining one integrated incident and breach evidence model.

3. Objectives

3.1 The objectives of this policy are to:

3.1.1 ensure suspected PII incidents are reported and recorded promptly;

3.1.2 ensure PII incidents are triaged and classified using consistent criteria;

3.1.3 ensure breach assessments consider affected PII, PII principals, systems, processing activities, processors, subprocessors, transfers, risks, and remedial actions;

3.1.4 ensure controller notification and PII principal communication decisions are documented;

3.1.5 ensure processor and subprocessor breach notifications to customers or upstream parties are made without undue delay and in accordance with applicable agreements;

3.1.6 ensure evidence is preserved and protected during incident handling;

3.1.7 ensure containment, eradication, recovery, and validation are tracked through REG10;

3.1.8 ensure regulated, contractual, customer, and sectoral reporting triggers are evaluated where applicable;

3.1.9 ensure incident lessons learned result in corrective action and continual improvement;

3.1.10 ensure incident and breach records are available for audit, management review, customer assurance, and regulatory review where applicable.

4. Policy Statements

4.1 Incident readiness and intake

4.1.1 [Both] The Privacy Lead / PIMS Manager MUST maintain PII incident and breach handling criteria in REG10 at least annually and after any material change to PIMS scope, legal context, contractual obligations, or high-risk processing.

4.1.2 [All] The Incident Response Coordinator MUST record every reported or detected suspected PII incident in REG10 within one business day of receipt, or sooner where an applicable notification or customer reporting timeline may be triggered.

4.1.3 [Both] The System Owner / Application Owner MUST preserve relevant system logs, alerts, access records, configuration evidence, and recovery evidence linked to REG10 when a suspected incident affects a system or application processing PII.

4.1.4 [Both] The Information Security Lead MUST complete initial technical triage of any security event involving PII within 24 hours of detection and record the initial severity, affected assets, and containment status in REG10.

4.2 Classification and breach assessment

4.2.1 [Both] The Incident Response Coordinator MUST classify each REG10 entry as a non-PII event, suspected PII incident, confirmed PII incident, or confirmed PII breach within 24 hours of intake or update the REG10 record with the reason classification remains pending.

4.2.2 [Both] The Privacy Lead / PIMS Manager MUST identify the affected processing activity, PII categories, PII principal categories, systems, processors, subprocessors, transfer locations, and privacy risks in REG02, REG04, REG08, REG09, and REG10 before the breach notification decision is finalized.

4.2.3 [Controller] The Data Protection Officer / Privacy Advisor MUST assess the risk to affected PII principals for each confirmed or reasonably suspected PII breach and record the notification recommendation, risk rationale, and advice in REG10 before the external notification decision is made.

4.2.4 [Processor] The Privacy Lead / PIMS Manager MUST identify the affected controller or customer and applicable contractual notification requirements as soon as the organization becomes aware of a PII breach affecting customer PII, and MUST record the outcome in REG08 and REG10.

4.2.5 [Joint Controller] The Privacy Lead / PIMS Manager MUST verify the agreed breach responsibility, lead communication responsibility, and coordination arrangement before any external notification or communication by a joint controller, and MUST record the decision in REG08 and REG10.

4.2.6 [Conditional] The Privacy Lead / PIMS Manager MUST evaluate applicable legal, sectoral, financial-sector, cybersecurity, contractual, customer, and service-recipient reporting triggers for each high-impact PII incident and record the applicability outcome in REG01, REG08, and REG10.

[... 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 [Both] The Privacy Lead / PIMS Manager MUST record any exception to this policy in REG12 before implementation, or within 24 hours after emergency action where prior approval was not feasible.

9.1.2 [Both] Top Management MUST approve any exception that materially affects breach notification timing, public communication, customer commitment, evidence preservation, or PII

principal risk before the incident is closed, with approval evidence retained in REG10 and REG12.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST document advice for any delayed notification, no-notification decision, or exceptional communication approach before incident closure, with advice retained in REG10.

9.1.4 [Both] The Vendor / Procurement Owner MUST record supplier, processor, subprocessor, or customer-driven exceptions affecting incident response in REG08 and REG12 within five business days of identifying the exception.

10. Enforcement

10.1.1 [All] The Process Owner / Business Owner MUST escalate failure to report a suspected PII incident, preserve evidence, follow assigned actions, or cooperate with breach assessment to the Privacy Lead / PIMS Manager within two business days of discovery, with evidence retained in REG12.

10.1.2 [Both] The Privacy Lead / PIMS Manager MUST record a REG12 nonconformity when a breach of this policy affects incident intake, triage, containment, notification, evidence integrity, communication, or corrective action.

10.1.3 [Both] The Vendor / Procurement Owner MUST initiate supplier or processor remediation through REG08 and REG12 within five business days when a processor, subprocessor, supplier, or other third party fails to meet agreed incident or breach obligations.

10.1.4 [Both] Top Management MUST review material or recurring incident-management nonconformities at the next scheduled management review, with decisions and required actions retained in REG12.

11. Review and Maintenance

11.1.1 [Both] The Privacy Lead / PIMS Manager MUST review this policy at least annually and record the review outcome, required changes, and approval status in REG12.

11.1.2 [Both] The Incident Response Coordinator MUST trigger a post-incident review of this policy within 30 calendar days after closure of any high-impact PII incident or confirmed PII breach, with review evidence retained in REG10 and REG12.

11.1.3 [Conditional] The Privacy Lead / PIMS Manager MUST review this policy within 30 calendar days of becoming aware of a material change to applicable legal, sectoral, customer, contractual, processor, subprocessor, or transfer-related incident reporting requirements, with review evidence retained in REG01, REG08, REG09, and REG12.

11.1.4 [Both] The Internal Audit / Compliance Reviewer MUST review implementation of this policy at least annually through the PIMS internal audit programme, with audit findings and corrective actions retained in REG12.

11.1.5 [Both] Top Management MUST review incident trends, significant breaches, notification performance, overdue corrective actions, and policy effectiveness during scheduled management review, with outputs retained in REG12.

12. Related Policies

12.1 This policy should be read with:

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 PII06 - PII Principal Rights Management Policy

12.7 PII07 - Privacy Risk Assessment and DPIA Policy

12.8 PII08 - Privacy by Design and Default Policy

12.9 PII10 - PII Retention, Deletion and Disposal Policy

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

12.11 PII13 - International PII Transfer Policy

12.12 PII14 - PII Security and Access Control Policy

12.13 PII16 - Privacy Training, Awareness and Competence Policy

12.14 PII17 - PIMS Documented Information and Evidence Management Policy

12.15 PII18 - PIMS Monitoring, Audit and Improvement Policy

13. Reference Standards and Frameworks

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.7; 4.5.1; 4.5.3; 4.5.4; 5.2.2; 6.2.2; 7.1.1; 7.1.7; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.2.2; 4.3.4; 4.6.3; 6.3.1; 7.1.4; 11.1.2].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 6.4.1; 6.5.1; 8.1.1; 8.1.4; 10.1.2; 11.1.4; 11.1.5].

13.4 ISO/IEC 27701:2025 - Annex A.3.11. Addressed by clauses [4.1.1; 4.1.2; 4.2.6; 4.4.1; 5.1.1; 5.4.1; 7.1.1; 7.1.2; 7.1.6].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.4; 4.2.1; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.3; 4.4.4; 4.5.1; 4.5.4; 6.3.1].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.2.6; 4.4.6; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.4; 6.2.2; 9.1.2; 11.1.3].

13.7 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.6. Addressed by clauses [4.2.4; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.2; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 4.6.2; 5.2.1; 6.3.1; 8.1.3; 11.1.5].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.1; 4.4.3; 5.3.1; 6.2.2; 11.1.3].

13.10 GDPR - Article 28. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.11 GDPR - Article 32. Addressed by clauses [4.1.3; 4.1.4; 4.3.2; 4.3.3; 4.5.2; 4.6.3; 5.5.1; 7.1.4; 8.1.2; 11.1.2].

13.12 GDPR - Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.1; 4.5.4; 8.1.3; 9.1.3].

13.13 GDPR - Article 34. Addressed by clauses [4.2.3; 4.2.5; 4.4.2; 4.4.3; 4.4.7; 4.5.4; 8.1.3; 9.1.3].

13.14 GDPR - Article 39. Addressed by clauses [4.2.3; 4.4.2; 5.3.1; 6.2.2; 9.1.3; 11.1.3].

13.15 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.2.2; 4.3.2; 4.3.3; 4.5.3; 4.6.2; 4.6.3; 5.2.2; 6.4.1; 8.1.4; 11.1.4].

13.16 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.3; 4.6.5; 7.1.3; 7.1.6].

13.17 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.5.1; 4.5.2; 4.6.1; 4.6.2; 7.1.2; 7.1.6].

13.18 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.2; 4.6.1; 5.4.1; 7.1.6; 11.1.2].

13.19 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.1; 4.6.1; 4.6.5; 5.1.1; 7.1.1; 7.1.3; 7.1.6; 8.1.6; 11.1.1; 11.1.2].

13.20 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.4; 4.5.1; 5.4.2; 6.1.2; 8.1.2].

13.21 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5].

13.22 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.2.6; 4.4.6; 4.4.7; 5.3.1; 6.2.2; 8.1.3; 11.1.3].

13.23 DORA Regulation (EU) 2022/2554 - Article 17; Article 18; Article 19. Addressed by clauses [4.2.1; 4.2.6; 4.4.6; 4.4.7; 5.1.2; 6.2.1; 8.1.3; 11.1.3; 11.1.5].