					Insert Registered Legal Entity Name Here							
Document number: PII14					Document Title: **PII Security and Access Control 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**

Legal Notice (Copyright & Usage Restrictions)

(C) 2025 Clarysec LLC. All rights reserved.

This document is the intellectual property of Clarysec LLC. No part may be copied, reused, redistributed, or modified for commercial or implementation purposes without explicit written permission.
Unauthorized use is strictly prohibited and may lead to legal action.
For licensing, contact: info@clarysec.com

Aligned with standards and regulations

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 6.1.3; Clause 8.1	Both	Primary	PII security control planning and operation
ISO/IEC 27701:2025	Clause 7.5; Clause 9.1; Clause 10.2	Both	Supporting	Evidence, monitoring and corrective action
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9	Both	Primary	Identity and access rights for PII processing
ISO/IEC 27701:2025	Annex A.3.22; Annex A.3.23	Both	Primary	Endpoint protection and secure authentication
ISO/IEC 27701:2025	Annex A.3.25; Annex A.3.26	Both	Primary	Logging and cryptographic protection
ISO/IEC 27701:2025	Annex A.3.28; Annex A.3.29	Both	Supporting	Application security and secure architecture
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.15; Annex A.3.16	Both	Supporting	Record protection and review
GDPR	Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32	Both	Primary	Security, accountability and processor controls
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	ISMS control integration
ISO/IEC 27002:2022	Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Security-control implementation guidance
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Information security and privacy compliance principles
ISO/IEC 29151:2022	Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5;	Both	Supporting	PII protection security controls

	Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4			

1. Scope

1.1 This policy defines PII-specific security and access control requirements for systems, applications, services, devices, cloud environments and operational processes that store, transmit, process, access, administer or protect PII.

1.2 This policy applies to controller, joint controller, processor and subprocessor contexts where the organization determines, operates, supports or relies on security controls for PII processing.

1.3 This policy covers the following PII security control domains:

1.3.1 PII security baseline and integration with existing information security policies;

1.3.2 access control;

1.3.3 authentication;

1.3.4 privileged access;

1.3.5 encryption and secure storage;

1.3.6 logging and monitoring;

1.3.7 secure configuration and vulnerability management;

1.3.8 endpoint and cloud access controls;

1.3.9 evidence linkage through REG02, REG08, REG10 and REG12.

1.4 This policy does not replace a full information security management system, network security policy, secure development policy, backup policy, endpoint policy, cloud security policy, cryptographic standard, vulnerability management procedure or incident response procedure. Where those policies already exist, this policy defines the PII-specific linkage and evidence requirements needed for PIMS assurance.

1.5 This policy does not duplicate:

1.5.1 PII processing inventory and lawful basis ownership in PII03;

1.5.2 privacy risk and DPIA methodology in PII07;

1.5.3 privacy by design gates in PII08;

1.5.4 collection, use, disclosure and sharing rules in PII09;

1.5.5 retention, deletion and disposal execution in PII10;

1.5.6 processor lifecycle governance in PII12;

1.5.7 international transfer mechanism controls in PII13;

1.5.8 incident and breach workflow in PII15;

1.5.9 documented information governance in PII17;

1.5.10 PIMS monitoring, audit and improvement governance in PII18.

1.6 For this policy, operational logs, security tool outputs, access review exports, vulnerability reports and configuration evidence are evidence sources that are attached to, summarized in, or referenced by the canonical evidence objects. They are not separate PIMS registers.

2. Purpose

2.1 The purpose of this policy is to ensure that PII is protected by appropriate, risk-aligned and auditable security and access controls throughout processing.

2.2 This policy enables the organization to demonstrate that PII security controls are planned, implemented, reviewed, monitored and improved through REG02, REG08, REG10 and REG12 without creating duplicate security registers or replacing existing information security policies.

3. Objectives

3.1 The objectives of this policy are to:

3.1.1 define a PII access control baseline for systems and processing activities;

3.1.2 ensure that authentication controls are appropriate to the sensitivity and access context of PII;

3.1.3 define review requirements for privileged and ordinary access to PII;

3.1.4 define encryption and secure storage expectations for PII at rest, in transit and in relevant cloud or endpoint contexts;

3.1.5 define logging and monitoring expectations for access to, changes to and administration of PII;

3.1.6 define secure configuration and vulnerability evidence requirements for systems processing PII;

3.1.7 define endpoint and cloud access expectations without creating a full endpoint or cloud security policy;

3.1.8 link suspected PII security incidents to REG10 without duplicating the incident workflow;

3.1.9 integrate with existing information security policies where available;

3.1.10 maintain audit-ready evidence using only REG02, REG08, REG10 and REG12.

4. Policy Statements

4.1 PII security baseline and ISMS integration

4.1.1 [Both] The Information Security Lead MUST define the PII security baseline for each system or service that processes PII in REG12 before the system or service enters production or materially changes.

4.1.2 [Both] The System Owner / Application Owner MUST record the implemented PII security-control evidence location in REG12 before relying on an existing information security control for PIMS assurance.

4.1.3 [Controller] The Process Owner / Business Owner MUST identify the PII sensitivity, processing context and access need in REG02 before requesting new or materially changed access to PII.

4.1.4 [Processor] The Vendor / Procurement Owner MUST record customer security instructions, customer responsibility boundaries and processor security commitments in REG08 before processor access to customer PII begins or materially changes.

4.1.5 [Both] The Privacy Lead / PIMS Manager MUST verify that PII security evidence is linked to REG02, REG08, REG10 or REG12 before accepting the processing activity as PIMS-auditable.

4.2 Access control baseline

4.2.1 [Both] The System Owner / Application Owner MUST restrict access to PII to approved roles and authorized users recorded or traceable in REG02 or REG12 before access is enabled.

4.2.2 [Both] The Process Owner / Business Owner MUST approve the business purpose for PII access in REG02 or REG12 before the System Owner / Application Owner provisions access.

4.2.3 [Both] The System Owner / Application Owner MUST review user access to systems processing high-impact or sensitive PII at least quarterly and record the review outcome in REG12.

4.2.4 [Both] The System Owner / Application Owner MUST review user access to other systems processing PII at least annually and record the review outcome in REG12.

4.2.5 [Both] The System Owner / Application Owner MUST remove or amend PII access in REG12 within one business day after role change, termination, contract completion or access no longer being required.

4.2.6 [Processor] The Vendor / Procurement Owner MUST confirm in REG08 that processor access to customer PII is limited to documented customer instructions before access is enabled or changed.

4.2.7 [Subprocessor] The Vendor / Procurement Owner MUST confirm in REG08 that subprocessor access to PII is limited to authorized subprocessing activities before subprocessor access is enabled or changed.

[... 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 Information Security Lead MUST record each exception to a PII security or access-control requirement in REG12 before the exception is activated.

9.1.2 [Both] The Data Protection Officer / Privacy Advisor MUST advise on higher-risk PII security exceptions in REG12 before approval.

9.1.3 [Both] Top Management MUST approve PII security exceptions in REG12 before activation when the exception affects high-impact PII, sensitive PII, privileged access, encryption, logging or unresolved high-risk vulnerabilities.

9.1.4 [Both] The Information Security Lead MUST define exception expiry, compensating control and review date in REG12 before exception approval.

9.1.5 [Both] The System Owner / Application Owner MUST remediate, renew or close expired PII security exceptions in REG12 within five business days after expiry.

9.1.6 [Processor] The Vendor / Procurement Owner MUST record processor or subprocessor security exceptions affecting customer PII in REG08 and REG12 before acceptance.

10. Enforcement

10.1.1 [Both] The Privacy Lead / PIMS Manager MUST record nonconformities for missing or incomplete PII security evidence in REG12 within five business days of identification.

10.1.2 [Both] The Information Security Lead MUST assign remediation ownership for PII security-control failures in REG12 within five business days of validation.

10.1.3 [Both] The System Owner / Application Owner MUST disable or restrict unauthorized, excessive or unsupported PII access within one business day of validation and record the action in REG12.

10.1.4 [Conditional] The Incident Response Coordinator MUST link enforcement actions to REG10 within one business day when the enforcement matter involves a suspected or confirmed PII incident.

10.1.5 [Both] Top Management MUST review repeated or high-risk PII security nonconformities in REG12 before management review.

11. Review and Maintenance

11.1.1 [All] The Privacy Lead / PIMS Manager MUST review this policy with the Information Security Lead at least annually and record the review outcome in REG12.

11.1.2 [Both] The Information Security Lead MUST review the PII security baseline in REG12 within 30 days after a material technology, threat, audit, incident or regulatory change affecting PII security.

11.1.3 [Both] The System Owner / Application Owner MUST update system-level PII security evidence in REG12 within 30 days after material architecture, access, configuration, vulnerability or logging change.

11.1.4 [Processor] The Vendor / Procurement Owner MUST review processor and subprocessor PII security responsibility evidence in REG08 within 30 days after material service, customer-instruction or subprocessor change.

11.1.5 [All] The Internal Audit / Compliance Reviewer MUST verify policy review evidence and selected PII security-control evidence in REG12 according to the approved audit plan.

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 PII07 - Privacy Risk Assessment and DPIA Policy;

12.6 PII08 - Privacy by Design and Default Policy;

12.7 PII09 - PII Collection, Use, Disclosure and Sharing Policy;

12.8 PII10 - PII Retention, Deletion and Disposal Policy;

12.9 PII12 - Processor, Subprocessor and Third-Party Privacy Management Policy;

12.10 PII13 - International PII Transfer Policy;

12.11 PII15 - PII Incident and Breach Management Policy;

12.12 PII16 - Privacy Training, Awareness and Competence Policy;

12.13 PII17 - PIMS Documented Information and Evidence Management Policy;

12.14 PII18 - PIMS Monitoring, Audit and Improvement Policy.

13. Reference Standards and Frameworks

13.1 ISO/IEC 27701:2025 - Clause 6.1.3; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.7; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5; 5.1.4; 5.1.6; 6.1.2; 7.1.1; 7.1.2].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.5.5; 4.6.3; 4.6.4; 4.7.5; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 7.1.3; 7.1.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.2; 11.1.1; 11.1.5].

13.3 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 10.1.3].

13.4 ISO/IEC 27701:2025 - Annex A.3.22; Annex A.3.23. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5].

13.5 ISO/IEC 27701:2025 - Annex A.3.25; Annex A.3.26. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.6 ISO/IEC 27701:2025 - Annex A.3.28; Annex A.3.29. Addressed by clauses [4.1.1; 4.1.2; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 7.1.1; 7.1.2].

13.7 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.15; Annex A.3.16. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.6.2; 4.6.3; 4.6.4; 4.7.2; 4.7.3; 5.1.9; 6.1.6; 8.1.4; 10.1.1; 11.1.5].

13.8 GDPR - Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.5; 4.2.6; 4.2.7; 4.3.2; 4.4.4; 4.5.1; 4.5.2; 4.6.1; 4.6.6; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 4.8.5; 5.1.1; 5.1.7; 6.1.4; 7.1.4; 9.1.3; 10.1.4].

13.9 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.10 ISO/IEC 27002:2022 - Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.11 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.1; 4.5.1; 4.6.2; 4.6.6; 4.7.6; 5.1.2; 6.1.1; 8.1.4; 10.1.1; 11.1.1].

13.12 ISO/IEC 29151:2022 - Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.7.1; 4.7.2; 4.7.4; 4.8.1; 4.8.2; 6.1.6; 11.1.5].