					Insert Registered Legal Entity Name Here							
Document number: PII24					Document Title: **CCTV and Physical Monitoring Privacy 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 7.5; Clause 8.1	Both	Primary	Documented and operational controls
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitoring and corrective action
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Purpose, lawful basis, risk trigger and records
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Processor and joint-controller allocation
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10	Controller	Supporting	PII principal obligations and requests
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Collection, processing, minimization, retention and disposal
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Disclosure records and requests
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Processor agreements, instructions, support and records
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Processor rights and disclosure support
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Records protection and logging
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Principles and accountability
GDPR	Article 6	Controller	Primary	Lawful basis
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Transparency and notices

GDPR	Article 15; Article 16; Article 17; Article 18; Article 21	Controller	Supporting	Rights requests
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Governance, processors, records, security, DPIA and advice
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Purpose, collection, minimization, retention and disclosure
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Transparency, participation, accountability, security and compliance
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Privacy risk and DPIA triggers
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	PII protection privacy controls
ISO/IEC 29151:2022	Clause 9.2.3; Clause 9.4.2; Clause 11.1.3	Both	Supporting	Access and physical entry controls
ISO/IEC 27002:2022	Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15	Both	Supporting	PII, physical monitoring, access restriction and logging

1. Scope

1.1 This policy applies to CCTV, video monitoring, visitor monitoring, physical access-control logs, guard-operated monitoring records, premises monitoring systems, and related physical monitoring activities that collect or otherwise process PII.

1.2 This policy applies to organizations acting as PII controllers for their own premises and physical monitoring activities. It also applies to processor or subprocessor support activities where the organization operates, hosts, reviews, stores, discloses, deletes, or otherwise processes monitoring footage, visitor data, or physical access logs on behalf of a customer.

1.3 This policy covers monitoring purpose definition, approval, notice and signage, access restrictions, disclosure, retention, deletion, outsourcing, incident escalation, rights request routing, review, and evidence management.

1.4 This policy does not provide employment-law advice, works-council legal commentary, law-enforcement procedure, or a dedicated CCTV register. Monitoring-specific evidence is maintained in the canonical PIMS evidence objects identified in this policy.

2. Purpose

2.1 The purpose of this policy is to establish privacy controls for CCTV and physical monitoring so that monitoring activities are purposeful, transparent, proportionate, access-controlled, retained for defined periods, disclosed only through approved channels, and supported by auditable PIMS evidence.

2.2 This policy supports consistent handling of monitoring footage, visitor records, physical access logs, and related monitoring PII without creating additional registers, committees, dashboards, or non-canonical roles.

3. Objectives

3.1 The objectives of this policy are to:

3.1.1 define monitoring purposes and processing scope before monitoring begins;

3.1.2 document CCTV, physical access, visitor monitoring, and physical monitoring activities in REG02;

3.1.3 identify monitoring activities that require privacy risk review or DPIA screening in REG04;

3.1.4 maintain transparent notice and signage evidence in REG07;

3.1.5 restrict access, viewing, export, disclosure, and retention of monitoring PII;

3.1.6 route PII principal requests through REG06;

3.1.7 manage outsourced monitoring providers and data-sharing evidence through REG08;

3.1.8 escalate suspected monitoring-related PII incidents through REG10;

3.1.9 record reviews, exceptions, nonconformities, corrective actions, audit findings, and improvements in REG12.

4. Policy Statements

4.1 Monitoring inventory, purpose, and approval

4.1.1 [Controller] The Process Owner / Business Owner MUST record each CCTV, visitor monitoring, physical access-control log, or physical monitoring activity in REG02 before the activity begins.

4.1.2 [Controller] The Privacy Lead / PIMS Manager MUST validate the REG02 entry for purpose, lawful basis, monitored location, PII categories, PII principal categories, retention, notice, access, and disclosure fields before activation of a new or materially changed monitoring activity.

4.1.3 [Controller] The Process Owner / Business Owner MUST record approved monitored zones, excluded zones, and collection boundaries in REG02 before cameras, sensors, visitor logs, or access-control logging are enabled.

4.1.4 [Conditional] The Process Owner / Business Owner MUST obtain a REG04 privacy risk decision before activating monitoring that involves systematic monitoring, audio recording, biometric identification, analytics-enabled detection, sensitive locations, vulnerable individuals, or non-obvious monitoring.

4.1.5 [Joint Controller] The Privacy Lead / PIMS Manager MUST record joint monitoring responsibility allocation in REG08 before shared monitoring with a landlord, facilities partner, customer, or other joint controller begins.

4.1.6 [Processor] The Privacy Lead / PIMS Manager MUST record customer monitoring instructions and permitted processing boundaries in REG08 before processing monitoring footage, visitor records, or physical access logs on behalf of a customer.

4.2 Notice and transparency

4.2.1 [Controller] The Process Owner / Business Owner MUST ensure monitoring signage or equivalent just-in-time notice evidence is recorded in REG07 before monitored areas are opened to PII principals.

4.2.2 [Controller] The Privacy Lead / PIMS Manager MUST link each monitoring notice in REG07 to the corresponding REG02 processing purpose before publication or material change.

4.2.3 [Processor] The Privacy Lead / PIMS Manager MUST provide monitoring notice-support information in REG08 when the organization operates monitoring services under customer instructions.

4.2.4 [Conditional] The Process Owner / Business Owner MUST record alternative transparency measures in REG07 and REG04 before non-obvious or emergency monitoring is activated.

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

9. Exceptions

9.1 [All] The Privacy Lead / PIMS Manager MUST record each exception to this policy in REG12 before the exception is used.

9.2 [Conditional] The Data Protection Officer / Privacy Advisor MUST document privacy advice in REG04 or REG12 before approval of exceptions involving non-obvious monitoring, audio recording, biometric identification, analytics-enabled monitoring, or sensitive monitoring locations.

9.3 [All] Top Management MUST approve exceptions exceeding 90 days in REG12 before extension beyond the initial exception period.

9.4 [All] The Privacy Lead / PIMS Manager MUST review open monitoring exceptions in REG12 at least monthly until closure.

10. Enforcement

10.1 [All] The Privacy Lead / PIMS Manager MUST record monitoring control failures as nonconformities in REG12 within five business days of confirmation.

10.2 [Both] The Information Security Lead MUST suspend unauthorized monitoring-system access within one business day of confirmation and record the action in REG10 or REG12.

10.3 [All] Top Management MUST assign corrective action ownership in REG12 within 10 business days for repeated or material policy violations.

10.4 [Conditional] The Incident Response Coordinator MUST initiate the PII incident workflow in REG10 upon suspected unauthorized disclosure, loss, or compromise of monitoring PII.

11. Review and Maintenance

11.1 [All] The Privacy Lead / PIMS Manager MUST review this policy and related monitoring evidence in REG12 at least annually.

11.2 [Controller] The Process Owner / Business Owner MUST revalidate each active monitoring purpose, notice, location scope, and retention entry in REG02 and REG07 at least annually.

11.3 [Both] The System Owner / Application Owner MUST revalidate monitoring-system access, logging, deletion, and export controls in REG12 at least annually and after material system change.

11.4 [Conditional] The Vendor / Procurement Owner MUST revalidate outsourced monitoring-provider evidence in REG08 at least annually and before contract renewal.

11.5 [All] The Privacy Lead / PIMS Manager MUST update related REG02, REG04, REG07, REG08, REG10, or REG12 evidence within 30 calendar days after approved policy changes.

12. Related Policies

12.1 PII02 - Privacy Roles, Responsibilities and Accountability Policy

12.2 PII03 - PII Processing Inventory and Lawful Basis Policy

12.3 PII04 - Privacy Notice and Transparency Policy

12.4 PII06 - PII Principal Rights Management 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 PII14 - PII Security and Access Control Policy

12.12 PII15 - PII Incident and Breach Management Policy

12.13 PII17 - PIMS Documented Information and Evidence Management Policy

12.14 PII18 - PIMS Monitoring, Audit and Improvement Policy

12.15 PII19 - Employee Privacy Policy

12.16 PII21 - AI and Automated Decision-Making Privacy Policy

12.17 PII23 - Cloud PII Processor 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 7.5; Clause 8.1** - Mapped to documented monitoring evidence, operational planning, activation controls, purpose records, notice linkage, access configuration, retention configuration, and change control for CCTV and physical monitoring activities. Addressed by clauses [4.1.1; 4.1.2; 4.2.2; 4.3.1; 4.4.1; 6.2; 7.1; 11.5].

13.2.2 **Clause 9.1; Clause 10.2** - Mapped to monitoring control measurement, provider review, access review, audit findings, nonconformities, corrective actions, overdue action escalation, and improvement evidence. Addressed by clauses [4.6.4; 6.4; 6.5; 6.6; 8.1; 8.7; 10.1; 11.1].

13.2.3 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9** - Mapped to controller monitoring purpose definition, lawful basis documentation, privacy risk trigger decisions, and records of monitoring processing activities in REG02 and REG04. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.4.1; 6.2; 7.1; 11.2].

13.2.4 **Annex A.1.2.7; Annex A.1.2.8 -** Mapped to outsourced monitoring provider allocation, joint monitoring responsibility allocation, and processor or joint-controller evidence in REG08. Addressed by clauses [4.1.5; 4.6.1; 4.6.2; 5.7; 6.2; 7.6].

13.2.5 **Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10** - Mapped to monitoring-related PII principal obligations, request routing, preservation needed to assess requests, and governance evidence for rights support. Addressed by clauses [4.5.1; 4.5.2; 5.2; 7.2; 11.5].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9** - Mapped to limiting monitoring collection, processing boundaries, minimization, retention periods, deletion, overwriting, retention holds, and extracted copy control. Addressed by clauses [4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 7.3; 7.5; 8.4].

13.2.7 **Annex A.1.5.4; Annex A.1.5.5** - Mapped to records of external disclosure, disclosure request handling, minimization before disclosure, and incident-linked disclosures involving monitoring PII. Addressed by clauses [4.3.4; 4.5.4; 7.8; 10.4].

13.2.8 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7** - Mapped to processor customer instructions, permitted processing boundaries, notice support, retention and deletion instructions, rights assistance, and processor records for outsourced monitoring services. Addressed by clauses [4.1.6; 4.2.3; 4.4.5; 4.5.3; 4.6.3].

13.2.9 **Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Mapped to processor support for customer obligations, disclosure authorization, disclosure records, notification of disclosure requests, and legally binding disclosure handling for monitoring PII. Addressed by clauses [4.3.5; 4.5.3; 4.6.2; 4.6.3].

13.2.10 **Annex A.3.14; Annex A.3.25** - Mapped to protection of monitoring records, restricted access, privileged access review, access logging, unauthorized access containment, and logging evidence for monitoring systems. Addressed by clauses [4.3.2; 4.3.3; 4.5.5; 5.4; 7.4; 10.2; 11.3].

13.3 GDPR

13.3.1 **Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)** - Mapped to lawfulness, fairness, transparency, purpose limitation, data minimization, storage limitation, and accountability evidence for monitoring activities. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.1; 4.4.2; 4.4.3; 6.1; 8.1; 11.2].

13.3.2 Article 6 - Mapped to lawful basis documentation for CCTV, visitor monitoring, physical access logs, and other physical monitoring activities. Addressed by clauses [4.1.2; 4.1.4; 7.1].

13.3.3 **Article 12; Article 13; Article 14** - Mapped to transparent monitoring notices, signage evidence, notice linkage to processing purposes, processor notice-support information, and alternative transparency measures. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 7.2; 8.2; 11.2].

13.3.4 **Article 15; Article 16; Article 17; Article 18; Article 21** - Mapped to access, rectification, erasure, restriction, objection, request routing, preservation needed to assess requests, and monitoring-related customer assistance. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 7.8; 11.5].

13.3.5 **Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39** - Mapped to controller governance, joint-controller allocation, processor governance, records of processing, security of monitoring systems, privacy risk review, DPIA triggers, and privacy advice. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 4.3.2; 4.3.3; 4.5.4; 4.6.1; 4.6.2; 4.6.4; 5.1; 5.3; 6.3; 8.5; 10.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Mapped to purpose specification, collection limitation, data minimization, use limitation, retention limitation, and disclosure

limitation for monitoring PII. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.4; 4.4.1; 4.4.2; 4.4.4; 7.8].

13.4.2 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12** - Mapped to transparency, individual participation, accountability, information security, compliance review, access review, rights routing, incident escalation, and corrective action evidence. Addressed by clauses [4.2.1; 4.2.2; 4.3.2; 4.3.3; 4.5.1; 4.5.4; 6.1; 8.7; 10.1].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 5.1; Clause 6.2** - Mapped to privacy risk and DPIA trigger screening for systematic, non-obvious, audio, biometric, analytics-enabled, sensitive-location, vulnerable-individual, or other higher-risk physical monitoring. Addressed by clauses [4.1.4; 4.2.4; 5.3; 6.3; 7.5; 9.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10** - Mapped to PII protection controls for purpose, collection, minimization, retention, disclosure, and PII principal participation in monitoring contexts. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.4.1; 4.4.3; 4.5.1; 7.2; 8.2].

13.6.2 **Clause 9.2.3; Clause 9.4.2; Clause 11.1.3** - Mapped to access provisioning, information access restriction, and physical entry controls relevant to monitoring-system access and physical access-control records. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.5.5; 5.4; 7.4; 10.2; 11.3].

13.7 ISO/IEC 27002:2022

13.7.1 Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15 - Mapped to privacy and protection of PII, physical entry, physical security monitoring, privileged access, information access restriction, and logging controls for CCTV and physical monitoring systems. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.5.5; 5.4; 7.3; 7.4; 8.3; 10.2; 11.3].