



An Garda Síochána

Ag Coinneáil Daoine Sábháilte - Keeping People Safe

TECHNICAL SPECIFICATION FOR AUTHORISATION AND INSTALLATION AND OPERATION OF CCTV FOR PARTICULAR PURPOSES

**Specifically, CCTV for The Sole
or Primary Purpose of Recording
a Public Place.**

**Part 5 of Garda Síochána
(Recording Devices) Act 2023**



Contents

1. Introduction	4
2. Overview, Legal Basis and Scope	4
2.1 Purpose of This Document	4
2.2 Legal Basis	5
2.3 Scope	5
2.4 Applicable Standards	5
2.5 Definitions	6
2.6 Public CCTV System Objectives.....	6
2.7 Guiding Principles.....	6
3. Governance, Roles, and Responsibilities	6
3.1 Contractors and System Integrators	6
3.2 Accountability and Documentation	7
4. Data Protection, Security and Operational Requirements	7
4.1 Physical Security	7
4.2 Cybersecurity Requirements.....	7
4.3 Incident Management	8
4.3.1 Security Incidents.....	8
4.3.2 Technical Failures	8
4.4 Vetting Requirements	9
4.5 Decommissioning	9
5. Technical Specification	9
5.1 General Requirements.....	9
5.2 Camera Requirements.....	10
5.2.1 General	10
5.2.2 Minimum Specification	10
5.3 Lens Requirements.....	10
5.4 Housing Requirements	10
5.5 Mounting Brackets	10
5.6 Camera Poles	11
5.7 CE Compliance.....	11
5.8 Recording and Storage	11
5.8.1 General	11

5.8.2 Minimum Recording	11
5.9 Video Management System (VMS) / Network Video Recorder (NVR)	11
5.10 Power Requirements	11
5.11 Environmental Requirements	12
5.12 Commissioning Requirements	12
5.13 Technical Integrity Requirements	12
5.14 Integration Requirements	12
6. Cloud-Based CCTV Systems	12
6.1 General Cloud Requirements	12
6.2 Deployment Models	13
6.3 Data Residency	13
6.4 Security Requirements	13
6.5 Availability and Resilience	13
6.6 Local Fail-Safe	13
7. Transmission Requirements	14
7.1 General Requirements	14
7.2 Fibre Optic Transmission	14
7.3 Microwave Transmission	14
7.4 IP Ethernet Radio	14
7.5 Wi-Fi	14
7.6 Encryption Requirements	14
7.7 Network Segmentation	15
7.8 Resilience	15
7.9 Documentation Requirements	15
8. System Monitoring	15
8.1 Health Monitoring	15
9. Services, Warranty and Maintenance	16
9.1 General Requirements	16
9.2 Warranty	16
9.3 Maintenance Contract	16
9.4 Upgrades	17
9.5 PSA Licensing	17
10. Artificial Intelligence (AI) and Analytics Governance	17

11. Appendices 18

 11.1 Glossary of Terms 18

 11.2 Technical Requirement Checklist 19

 11.3 System Commissioning Checklist 19

 11.4 Annual Audit to include:..... 19

 11.5 PSA Licensing Appendix 19

 11.6 System Documentation 20

CCTV Systems Recording in a Public Place

TECHNICAL SPECIFICATION FOR CCTV SYSTEMS

1. Introduction

This document is a technical specification required under the Garda Síochána (Recording Devices) Act 2023 (the Act). All legislative requirements should be borne in mind when referring to this document.

It is advisable that legal advice should be taken in relation to the Act to ensure all CCTV suppliers understand how non-compliance with the legislation could affect any authorisation issued by the Garda Commissioner.

Any equipment installed must reflect exactly the technology authorised by the Commissioner of An Garda Síochána. **Any breach of the legislation may cause a CCTV authorisation to be revoked.**

It is a legislative requirement that anyone installing, operating, or monitoring a CCTV system recording in a public place must have a contract with the Commissioner of An Garda Síochána or the Local Authority (the Owners) at that time. A CCTV system authorisation cannot exceed 5 years and must be renewed before expiration.

2. Overview, Legal Basis and Scope

2.1 Purpose of This Document

This document defines the minimum technical requirements for CCTV systems recording in a public place authorised under Part 5 of the Garda Síochána (Recording Devices) Act 2023. It is a Technical Specification and guidance on best practice around the installation and provision of CCTV systems.

The purpose of this document is to ensure CCTV systems:

- Operate lawfully and transparently.
- Meet evidential and technical integrity standards.
- Protect rights and freedoms.
- Support policing and crime prevention.
- Comply with the Code of Practice for Public Closed-Circuit Television (CCTV).
- Maintain secure and reliable infrastructure.

The intended audience is:

- Local Authorities.

- Contractors and system integrators.
- Garda Divisional Officers.
- Garda ICT.
- Technical assessors and auditors.

2.2 Legal Basis

Public CCTV systems must comply with:

- Garda Síochána (Recording Devices) Act 2023.
- Public CCTV Code of Practice.
- The authorisations of CCTV systems which last 5 years at which point authorisations are either renewed or removed.

Any technological change implemented without written approval of the Garda Commissioner invalidates the authorisation.

2.3 Scope

This document applies to:

- All CCTV systems recording in public places.
- All cameras, housings, poles, brackets used in the Public CCTV system.
- All CCTV transmission systems used in the CCTV system.
- All NVR/VMS used to manage and record CCTV Data.
- All CCTV data storage and monitoring equipment.
- All contractors and authorised personnel.

This document does not apply to:

- Private CCTV.
- CCTV on Garda premises.
- Body-worn cameras.
- ANPR (with the exception of ANPR enabled CCTV).
- Recording devices fitted to aerial platforms.

2.4 Applicable Standards

All systems should where possible comply with the following technical standards:

- EN 62676
- EN 62368-1
- ISO/IEC 27001:2022
- IEEE 802.3
- ONVIF Profiles S, G, T and M (latest profiles)

2.5 Definitions

Key terms:

- Recording Device.
- Media Storage Device.
- Public Place.
- Relevant Data.
- (Full glossary in Section 11).

2.6 Public CCTV System Objectives

The CCTV Systems design must support the purpose of Public CCTV as per Section 26 of the Act:

- the prevention, investigation, detection or prosecution of criminal offences,
- safeguarding against, and the prevention of, threats to public security, including securing public safety and public order, or
- the protection of the security of the State.

The CCTV systems must:

- comply with the legislation.
- be proportionate and transparent.

2.7 Guiding Principles

All systems must operate under the following seven key principles of Article 5 General Data Protection Regulation.

- Lawfulness, fairness, and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality; and
- Accountability.

3. Governance, Roles, and Responsibilities

3.1 Contractors and System Integrators

Contractors must:

- Hold valid PSA licence.
- Be Garda-vetted to the required level.
- Use CE-compliant equipment.

- Remove default credentials and passwords on all technical equipment installed.
- Provide as built documentation and keep it up to date for inspection.
- Maintain confidentiality.
- Contractors will (most likely) act as Data Processors and must sign written agreements to ensure Data Protection compliance.

3.2 Accountability and Documentation

The following must be maintained by the Contractor for evidential and audit purposes:

- Electronic Access logs – Electronic access logs should be kept at least 5 years.
- Maintenance logs.
- Configuration records.
- Cybersecurity records.
- A Security Assessment Sheet must be completed for all procurements and upgrades.
- Documentation must be retained for the duration of systems operation.

4. Data Protection, Security and Operational Requirements

4.1 Physical Security

The CCTV system equipment and technical design must protect against:

- Theft.
- Vandalism.
- Tampering.
- Unauthorised access.
- Storage theft by providing secure access-controlled cabinets.

4.2 Cybersecurity Requirements

All CCTV systems recording in a public place must implement layered cybersecurity controls in accordance with recognised international standards and current best practice.

The CCTV Systems must implement:

- AES-256 encryption (minimum) for all data at rest.
- TLS 1.3 minimum for all data in transit (TLS 1.2 only permitted for legacy interoperability where justified).
- Secure boot and signed firmware.
- Hardware root of trust where supported.

- Removal of all default passwords prior to commissioning.
- Mandatory multi-factor authentication (MFA) for all administrative access.
- Role-based access control (RBAC) with least privilege principles.
- Network segmentation using VLANs or equivalent.
- Firewall protection with explicit allow rules.
- Intrusion detection and/or intrusion prevention capability.
- Logging of all administrative and access events.
- Centralised log aggregation where feasible.
- Secure time synchronisation (authenticated NTP).

Vulnerability and Patch Management:

The system manager must implement a documented vulnerability management process. This process must include monitoring for security advisories, risk assessment of vulnerabilities, application of critical patches within 14 days, high severity patches within 30 days, and documented remediation tracking. This may not be as critical on standalone systems but if they are connected to Live networks or the internet then this is a critical requirement.

Unsupported or end-of-life equipment must not remain in service.

Supply Chain Security:

All hardware and software components must be sourced from reputable manufacturers and support secure firmware validation.

Manufacturers must provide security update commitments and vulnerability disclosure processes.

4.3 Incident Management

4.3.1 Security Incidents

Must be:

- Reported immediately.
- Logged.
- Investigated.
- Reported to DPC where required.

4.3.2 Technical Failures

Must be:

- Logged.
- Reported.
- Repaired.
- Documented.

4.4 Vetting Requirements

All personnel involved in installation, maintenance, monitoring, or access must be Garda-vetted.

4.5 Decommissioning

When a CCTV system is decommissioned:

- All recordings should be securely deleted in the agreed time-period.
- All storage devices must be destroyed and not reused.
- All CCTV signage should be removed.
- A decommissioning report should be prepared and forwarded to Garda National Community Engagement Bureau via the local Garda Divisional Officer.
- The Commissioner of An Garda Síochána should be informed in writing of the system decommissioning and the date it took effect.
- The Commissioner of An Garda Síochána can revoke authorisation for the Public CCTV as outlined in Section 32 of the Act.

5. Technical Specification

5.1 General Requirements

All CCTV systems recording in a public place must be designed as IP-based, digital, encrypted video surveillance systems.

Camera deployments must be designed using EN 62676-pixel density principles to ensure evidential suitability. Pixel density requirements:

Purpose	Minimum Pixels Per Metre
1. Identification	250ppm
2. Recognition	125ppm
3. Observation	62ppm
4. Detection	25ppm

Analogue CCTV systems may only be used where integration with legacy infrastructure is unavoidable and must still meet all minimum performance requirements. All CCTV systems must be designed with modular components to allow for future upgrades, such as higher resolution cameras or additional analytics if authorised later.

All CCTV Systems must be:

- IP-based.

- Digital.
- Encrypted.

5.2 Camera Requirements

5.2.1 General

- IP-based.
- Encrypted streams.
- Privacy masking is required on Static and PTZ cameras and must be capable of covering all required areas to be masked identified in the DPIA.
- All cameras should be capable of Secure updates.
- All Cameras should be mounted securely at 6–8-meter mounting height.

5.2.2 Minimum Specification

- 2 MP (1080p) minimum resolution (5MP preferred where operationally justified). The larger the resolution the higher the storage requirements.
- 25fps.
- H.265 / H.265+ (H.264 is also acceptable).
- WDR ≥ 140 dB true WDR.
- ONVIF S/G/T.
- IR capability.

5.3 Lens Requirements

Motorised zoom:

- F1.4.
- Auto iris.
- ND filter.
- Presets.
- <5s zoom.

5.4 Housing Requirements

Minimum:

- IP66/IP67.
- IK10.
- -30°C to $+50^{\circ}\text{C}$ Temperature spec should suit Irish weather extremes.
- Protect against rain, dust, insects, and impact.
- Support heaters, blowers, and wipers where required.
- Provide sealed cable entry points.

5.5 Mounting Brackets

- Corrosion-resistant.

- ≥800N wind rating.
- Anti-tamper.

5.6 Camera Poles

- Galvanised steel (Suppliers may have to take account of local street furniture design).
- 4mm wall thickness (Suggested only, supplier should use a design process to ensure safety).
- 6–8m height.

5.7 CE Compliance

All components must be CE compliant.

5.8 Recording and Storage

5.8.1 General

Suppliers need to carefully select

- NVR/VMS/Hybrid or Cloud solutions with a view to secure compatibility with other CCTV systems.
- Encrypted Data storage is required at Rest in transit and while in use.
- A proper audit logging process is required.

5.8.2 Minimum Recording

- 24/7 recording.
- 30-day retention.
- SHA-256 or SHA-3 hashing with export integrity verification.
- The CCTV system should be NTP synchronised or be synchronised using a GPS clock.

5.9 Video Management System (VMS) / Network Video Recorder (NVR)

The VMS/NVR Must support:

- Role-based access.
- Secure export.
- Audit logs.
- Multi-camera playback.

5.10 Power Requirements

- Surge protection.
- UPS backup.
- Lightning protection.

- POE.

5.11 Environmental Requirements

All external equipment must withstand:

- High winds.
- Rain.
- Salt exposure.
- Temperature changes.
- Irish Environmental Conditions.

5.12 Commissioning Requirements

The CCTV supplier must verify for the owner of the CCTV system the:

- The required masking of privacy locations.
- Image quality.
- Retention recording time.
- Cybersecurity stance of the system.
- Transmission network and encryption used.
- Camera placement is mapped correctly.

5.13 Technical Integrity Requirements

The CCTV supplier must protect against:

- Tampering.
- Interference.
- Data manipulation.
- Signal interception.

5.14 Integration Requirements

Legacy systems must be integrated with new CCTV systems securely.

6. Cloud-Based CCTV Systems

6.1 General Cloud Requirements

Cloud-based CCTV systems recording in a public place must comply with all provisions of the Garda Síochána (Recording Devices) Act 2023 and this Technical Specification.

Cloud systems must maintain evidential integrity, technical integrity, and data protection compliance equivalent to or exceeding on-premises systems.

6.2 Deployment Models

- On-Premises with encrypted cloud backup.
- Hybrid (Edge recording with encrypted replication to cloud).
- Fully Cloud-Hosted subject to written authorisation Commissioner of An Garda Síochána.

6.3 Data Residency

- All recordings stored in cloud environments must be stored within the European Union with a preference for Ireland.
- Cloud providers must provide confirmation of data routes, data centre locations and Data processors used for any data processing in the Cloud environment.
- All video streaming of video data must reside in the European Union.

6.4 Security Requirements

The general basis of security rests with using:

- AES-256 encryption at rest.
- AES-256 encryption in transit.
- TLS 1.3 minimum.
- Role-based access control.
- Mandatory multi-factor authentication.
- Full audit logging.
- Immutable storage capability (WORM where supported).

6.5 Availability and Resilience

The CCTV supplier must strive to have:

- Minimum 99.95% service availability (99.99% preferred).
- Redundant storage across availability zones.
- Documented disaster recovery procedures.

6.6 Local Fail-Safe

Fully cloud-hosted systems must provide minimum 24-hour local CCTV data buffering.

The supplier should where possible have a 6.X Cloud Incident Response:

Cloud providers must provide:

- Breach notification within 72 hours.
- Security incident escalation contacts.
- Documented incident handling procedures.
- Regular testing of incident response processes.

7. Transmission Requirements

7.1 General Requirements

- All transmission must be encrypted and IP-based.
- Copper/coax base-band transmission is not permitted.

7.2 Fibre Optic Transmission

Preferred method.

1. Single-mode fibre.
2. 10Gbps backbone preferred.
1Gbps minimum per camera aggregation switch.
3. Fusion splicing.
4. All Fibre routes should be documented.

7.3 Microwave Transmission

Only where fibre not feasible.

Must include:

- AES-256 encryption.
- ComReg.ie compliance.

7.4 IP Ethernet Radio

- ≥300 Mbps aggregate throughput.
- VPN tunnelling.
- AES-256.

7.5 Wi-Fi

Not recommended.

If used:

1. WPA3-Enterprise.
2. Encrypted.
3. Documented.

7.6 Encryption Requirements

All CCTV traffic must use:

- AES-256.
- TLS 1.3 minimum.
- IPsec/VPN.
- Unencrypted transmission prohibited.

7.7 Network Segmentation

A CCTV Supplier must use:

- VLANs.
- Firewalls.
- ACLs.

7.8 Resilience

A CCTV supplier must include:

- Surge protection.
- Redundant power.
- Health monitoring.

7.9 Documentation Requirements

The CCTV supplier must provide:

- As built Diagrams.
- Keep a record of all Licences and payment details.
- Encryption documentation.
- IP addressing scheme.
- 7.X Zero Trust Architecture.
- Continuous verification of access rights. As staff change and move credentials should be changed.
- Segmentation between camera groups and management interfaces.
- Certificate-based authentication as it is preferred over shared secrets.

8. System Monitoring

8.1 Health Monitoring

The CCTV system should where possible include and monitor:

- Disk health.
- Storage capacity.
- Camera connectivity.
- Transmission status.
- CPU/memory.
- Firmware status.
- Alerts must be logged and investigated.
- Cloud Connectivity.
- Video Stream.
- Video upload.

9. Services, Warranty and Maintenance

9.1 General Requirements

All CCTV Services provided by the contractor must comply with:

- this Technical Standards document.
- the Garda Síochána Public CCTV Code of Practice.
- the Garda Síochána (Recording Devices) Act 2023.
- be delivered by Valid PSA-licensed contractors.
- maintain the technical integrity and evidential reliability of the system.
- ensure continuous, secure, and lawful operation.
- PSA licensing.
- ensuring that the CCTV provider remains in full contract with the owner of the authorised CCTV system.

Documentation must be maintained recording all work performed.

NOTE Section 29 of the Garda Síochána (Recording Devices) Act, 2023 requires that any person installing or operating the authorised systems must have both a contract in place with the authorised body and have a written agreement in relation to the processing of data. All contractors should be familiar with Section 29 (1) of the Act.

9.2 Warranty

All CCTV suppliers should purchase a minimum 36-month warranty covering:

- Cameras.
- Housings.
- Storage.
- Housings and brackets.
- Poles and mounting hardware.
- Transmission equipment.
- Network switches and routers.
- NVR/VMS servers and storage.
- Power supplies and UPS units.
- Software and firmware.
- Installation workmanship.
- Cloud/Hybrid.

It is now a realistic possibility to get a 5-year warranty on most CCTV equipment which would last the full length of the effective CCTV Authorisation.

9.3 Maintenance Contract

The CCTV contract must include:

- An emergency response within 24 hours. Standard response of three working days for other less important outages or faults. The owner should seek the best response setup that suits their individual needs.
- A periodic preventative maintenance inspection programme (every 3 or 6 months) to ensure the equipment is working to all recommended standards.
- Reactive repairs.
- Cybersecurity updates.
- Privacy masking verification during all periodic Inspections to ensure Privacy masking is still in place as recommended.
- 99% annual availability.

As the CCTV system is authorised for 5 years and the relevant business owner (Garda / Local Authority) must have a contract in place with the CCTV supplier and it is recommended that a maintenance contract must be entered into for the five (5) years the system is authorised for.

9.4 Upgrades

All Software and hardware upgrades to the CCTV system must:

- Maintain performance.
- Maintain cybersecurity standards.
- Be documented.
- Follow change control.

9.5 PSA Licensing

All CCTV Contractors must:

- Hold valid PSA licence.
- Maintain Garda vetting.
- Provide proof of same if requested at any time.

10. Artificial Intelligence (AI) and Analytics Governance

AI is not currently sanctioned for use on publicly operated CCTV systems. No AI features can be switched on without the expressed written permission of the Garda Commissioner. All AI functionalities must be switched off by default on all equipment installed on the CCTV system.

If AI-enabled analytics are ever to be deployed, the CCTV systems must:

- Comply with applicable EU AI Act provisions.
- Provide documented transparency of analytics functionality.
- Avoid biometric identification unless separately authorised.

- Log analytics configuration changes.
- Provide human oversight capability.
- Be authorised in writing by the Garda Commissioner.

11. Appendices

11.1 Glossary of Terms

Term	Definition
Authorised Operator	As defined under Part 5 of the 2023 Act.
Data Controller	The Data Controller is any person who decides the purposes for which and how personal data is processed. An Garda Síochána and Local Authorities are a data controller for personal data processed within the scope and application of the Code of Practice.
Data Processor	A natural or legal person, public authority, agency or other body which processes data on behalf of the data controller
Operational Requirement	A documented justification for camera placement and system design.
DPIA	Data Protection Impact Assessment required under GDPR.
Public Place	This means a place to which the public have or are permitted access, whether as of right or by express or implied permission and whether subject to or free of charge.
Recording Device	Recording device means any of the following (a) a device or system that is capable of creating a record in any medium from which visual images (including moving visual images) or sounds, or both, may, by any means, be reproduced, (b) includes any devices or systems that are capable of processing the record made under paragraph (a), which may include— I. Reproducing by any means the visual images (including moving visual images) or sounds concerned,

	ii. using ANPR in respect of the record, or iii. producing a document relating to the record or the processing concerned. includes any device or system referred to in paragraph (a) or (b) that is in or affixed to a vehicle or a structure.
Principal Purposes	Principal purposes for operating a public closed-circuit television system are provided for in section 26 of the 2023 Act.
MCC	Monitoring Control Centre
NVR/VMS	Network Video Recorder / Video Management System.

11.2 Technical Requirement Checklist

Any checklist should include:

- Hardware & Infrastructure: Servers, workstations, and network requirements.
- Software & Platforms: Operating systems, browsers, and third-party tools.
- Data & Integration: Database requirements, APIs, data migration, and legacy system compatibility.
- Security & Compliance: SSL certificates, encryption, firewalls, and regulatory standards (GDPR, HIPAA, etc.).
- Performance & Scalability: Expected load (concurrent users), latency requirements, and response times.
- Usability & Accessibility: User interface standards, and compliance.

11.3 System Commissioning Checklist

All system commissioning should be documented using:

- Technical verification.
- Security verification.
- Documentation.

11.4 Annual Audit to include:

- Technical audit.
- Cybersecurity audit.

11.5 PSA Licensing Appendix

- Contractor obligations.

- Verification requirements.

11.6 System Documentation

Complete documentation set must include:

- As built design drawings.
- Transmission diagrams.
- Commissioning certificates.
- Maintenance logs.
- Audit logs.
- PSA documentation.