Surveillance System Deployment Checklist

The gate-by-gate checklist a team runs before a surveillance system goes live. Companion to the article. Verify each item on the installed system, at night and under load.

How to use it: five gates, six domains

Move through five gates - design, staging, installation, commissioning, go-live - and verify the six domains below at each. Do not pass a gate until the prior work is verified against written criteria. Commission at night and under load; 'online' is not 'recording', and untested redundancy is a hope.

1 Cameras & coverage

- [ ] Field of view & framing match the design, per camera
- [ ] Pixel-density / DORI target met in the real scene (IEC 62676-4)
- [ ] Night & backlit image verified on the recording, not the live view
- [ ] Privacy masking applied to areas you may not record

2 Network & power

- [ ] PoE budget >= camera demand + 30% headroom (per switch)
- [ ] Cameras on an isolated VLAN, behind a firewall, no internet route
- [ ] Aggregate bandwidth + uplink headroom sized for record + retrieval
- [ ] One NTP / GPS clock; every device agrees (evidential time)

3 Recording & storage

- [ ] Per-camera playback from the archive - not just 'online'
- [ ] Recording mode set per design (continuous / motion / event)
- [ ] Retention days verified against the storage math
- [ ] RAID / N+1 failover tested by causing a failure on purpose

4 Analytics

- [ ] Each analytic runs on the planned tier (edge / server / cloud)
- [ ] Tuned to a livable false-alarm rate - never '100% / zero false'
- [ ] Acceptance criteria written and met on the live scene
- [ ] BIOMETRIC GATE: lawful basis / consent (GDPR Art. 9 / BIPA)

5 Privacy & compliance

- [ ] Signage posted & privacy notice published (layered, EDPB 3/2019)
- [ ] DPIA completed and signed (large-scale / public monitoring)
- [ ] Retention auto-deletion set to the limit and tested (Art. 5(1)(e))
- [ ] Lawful basis / balancing test documented before go-live

6 Cybersecurity & operations

- [ ] Every default password changed (the #1 exploited weakness)
- [ ] Firmware patched; no open CISA advisories for the models
- [ ] Streams & management traffic encrypted where supported
- [ ] Per-user RBAC + audit logging on (who viewed / exported)

Go-live gate & operations - the deployment is not done until these are true

- [ ] FAT passed on the bench / in staging before shipping to site
- [ ] SAT passed: all six domains verified on the installed system
- [ ] NDAA 889 / FAR 52.204-25 supply-chain screen confirmed (where it applies)
- [ ] Handover package delivered: SAT report, as-builts & config, device/credential inventory, maintenance plan / SLA, operator training, known-issues list
- [ ] Health monitoring live: a camera that stops recording is alerted in hours
- [ ] First-30-days review scheduled to catch focus drift, seasonal-light misfires, retention behaviour under real load

Engineering guidance, not legal advice. Biometric analytics (face recognition; in many places licence-plate recognition) process special-category / biometric data restricted under GDPR Art. 9 and Illinois BIPA (740 ILCS 14, with a private right of action and statutory damages); notice, a DPIA, and retention limits (GDPR Art. 5(1)(e), Art. 13, Art. 35; EDPB Guidelines 3/2019) are go-live blockers. Confirm specifics with qualified counsel.