MPS 19 – Surveillance and Analysis

Category: Protection

Tags: surveillance, security operations, risk management, incident response, data protection, ISO27001, ISO18788, protection

Description: Minimum Performance Standard for Surveillance and Analysis. Defines the intent, required actions, and guidance for implementing risk-based, ethical, and effective surveillance systems that support loss prevention, incident response, regulatory compliance, and continuous improvement in any operational environment. Emphasises integration with broader security management systems, protection of data privacy, secure storage of surveillance data, and professional, qualified surveillance operations aligned with international standards such as ISO 27001, ISO 18788, and best-practice privacy frameworks.

Assessment Criteria (Structured)

1. 1.

Requirement: A Surveillance Policy or SOP must be documented, risk-based, approved, communicated, and reviewed annually.

Evidence: Signed policy or SOP document, communication logs, and review history.

2. 2.

Requirement: Risk assessments must inform camera placement, recording requirements, redundancy, and evidentiary standards.

Evidence: Risk assessment reports and camera placement plans.

3. 3.

Requirement: Surveillance facilities must have controlled access, secure infrastructure segregation, and log all entry.

Evidence: Access control logs and infrastructure layout documents.

4. 4.

Requirement: Only dedicated, trained, and qualified surveillance personnel may operate systems.

Evidence: Training records, qualifications, and role assignment logs.

5. 5.

Requirement: Personnel records must include training history, performance monitoring, and competency assessments.

Evidence: HR files, assessment forms, and evaluation records.

6. 6.

Requirement: Transfer-in/out of surveillance staff must follow approved protocols protecting operational integrity.

Evidence: Transfer records and authorisation forms.

7. 7.

Requirement: Surveillance training must include layout orientation, anomaly detection, and ethical behaviour.

Evidence: Training content and attendance logs.

8. 8.

Requirement: Annual data protection training must cover ethics, privacy laws, and internal policies.

Evidence: Training logs and compliance certificates.

9. 9.

Requirement: Comprehensive SOPs must define surveillance roles, shift protocols, escalation, and data protection.

Evidence: Approved SOP documents and user guidance files.

10. 10.

Requirement: A Quality Management System must support daily/weekly/monthly reporting audits and improvement actions.

Evidence: Review logs, audit trails, and CAPA reports.

11. 11.

Requirement: Surveillance planning must be risk-based and reflect evolving threats and conditions.

Evidence: Planning documents, updates, and approval logs.

12. 12.

Requirement: Operators must conduct regular facility orientation visits.

Evidence: Orientation schedules and participation records.

13. 13.

Requirement: Surveillance systems must integrate with incident management for consistent logging and analysis.

Evidence: Integration architecture, incident reports, and dashboards.

14. 14.

Requirement: Video review criteria must be documented with outcomes and follow-up action tracking.

Evidence: Review forms, logs, and outcome summaries.

15. 15.

Requirement: Interventions in high-risk areas must follow chain-of-custody protocols with secure storage.

Evidence: Custody forms, storage logs, and evidence tracking.

16. 16.

Requirement: Management must review surveillance activities through audits and oversight mechanisms.

Evidence: Audit reports, review records, and management dashboards.

17. 17.

Requirement: Real-time incident response procedures must include escalation and operator guidance.

Evidence: Response protocols and intervention templates.

18. 18.

Requirement: Non-compliance events must be addressed through documented protocols and displayed guidance.

Evidence: Incident forms, staff communications, and enforcement logs.

19. 19.

Requirement: Access to surveillance data must be controlled, authorised, and logged.

Evidence: Access logs, authorisation registers, and control policies.

20. 20.

Requirement: Surveillance data must be stored securely with backups, retention policies, and compliance alignment.

Evidence: Storage configurations, backup logs, and retention schedules.

21. 21.

Requirement: High-risk footage must be handled separately with audit trails and review mechanisms.

Evidence: Footage handling protocols and log entries.

22. 22.

Requirement: Surveillance technology must align with organisational integrity and privacy considerations.

Evidence: Technology guidance documents and privacy risk assessments.

23. 23.

Requirement: Monitoring practices must be communicated transparently to staff, contractors, and visitors.

Evidence: Communication records and consent documentation.

24. 24.

Requirement: Third-party/offsite surveillance arrangements must ensure secure data transfer and independence.

Evidence: Third-party contracts and SLA documentation.

25. 25.

Requirement: A liaison list must be maintained for secure engagement with regulators and law enforcement.

Evidence: Liaison lists and engagement records.