MPS 15 – Physical Security

Category: Protection

Tags: physical security, access control, surveillance, risk assessment, security philosophy, technology-first, data analytics, ISO 27001, ASIS, protection

Description: Minimum Performance Standard for Physical Security. Defines the intent, required actions, and guidance for establishing risk-based, layered physical security measures that prioritise technology-led controls, integrate human-based processes as supportive layers, and create data-rich environments for monitoring, analysis, and continuous improvement. Aligns with ASIS Physical Asset Protection Standards and ISO 27001 Physical Security requirements to ensure security systems are designed to deter, detect, delay, and respond to threats while supporting resilience and safety.

Assessment Criteria (Structured)

1. 1.

Requirement: An approved Security Philosophy must articulate principles and objectives, prioritising technology-first layered controls.

Evidence: Signed document outlining foundational security philosophy and supporting principles.

2. 2.

Requirement: A Physical Security Policy must align with the approved philosophy and be accessible, communicated, and reviewed regularly.

Evidence: Policy documents, review schedules, and internal communication records.

3. 3.

Requirement: Physical Security Procedures must align with policy, be approved, communicated to staff, and monitored for compliance.

Evidence: Procedure manuals, staff acknowledgment records, and compliance reports.

4. 4.

Requirement: Risk assessments must inform the design of physical security systems, identifying threats and vulnerabilities.

Evidence: Completed risk assessments, threat matrices, and design inputs.

5. 5.

Requirement: A threat matrix or risk register must be maintained and updated with stakeholder input and mitigation strategies.

Evidence: Risk register, update logs, and stakeholder meeting minutes.

6. 6.

Requirement: Risk mitigation action plans must be defined, tracked, and show demonstrable outcomes.

Evidence: Mitigation plans, tracking logs, and implementation status updates.

7. 7.

Requirement: Technical controls must serve as the primary security layer, including access control, CCTV, alarms, and biometrics.

Evidence: System inventories, specifications, and operational testing logs.

8. 8.

Requirement: Human-based controls must supplement technical systems for monitoring, manual verification, and response.

Evidence: Guard post procedures, manual verification logs, and response SOPs.

9. 9.

Requirement: Security systems must be designed as data-rich environments supporting real-time monitoring and analytics.

Evidence: System integration diagrams, logging features, and analytics platform screenshots.

10. 10.

Requirement: Security data must integrate with broader organisational analytics to inform risk decisions.

Evidence: Evidence of data pipelines, dashboards, and cross-functional reports.

11. 11.

Requirement: Access control systems must include electronic authorisation and full audit trails.

Evidence: Access logs, biometric scans, and audit reports.

12. 12.

Requirement: Access and egress patterns must be recorded and reviewed for personnel, vehicles, and materials.

Evidence: Tracking reports, exception reports, and investigation logs.

13. 13.

Requirement: Security zoning and layered protection strategies must be clearly defined and documented.

Evidence: Site layouts, access level matrices, and boundary maps.

14. 14.

Requirement: Surveillance systems must be deployed based on risk assessments and include alerting capabilities.

Evidence: CCTV coverage maps, alert logs, and functional checklists.

15. 15.

Requirement: Monitoring systems must support continuous recording and incident playback.

Evidence: Recording system logs and playback capability confirmations.

16. 16.

Requirement: Quality assurance processes must verify installation, configuration, and operational readiness.

Evidence: QA checklists, commissioning reports, and approval records.

17. 17.

Requirement: Electronic key and lock systems must integrate with access control and include audit trails.

Evidence: Key system configurations and audit history.

18. 18.

Requirement: Seal management protocols must be documented with issuance, verification, and reporting procedures.

Evidence: Seal logs, verification checklists, and audit summaries.

19. 19.

Requirement: Search procedures must prioritise advanced technologies such as x-ray or millimetre-wave scanners.

Evidence: Search protocols, equipment inventories, and usage logs.

20. 20.

Requirement: Training must demonstrate staff competency in search, surveillance use, and incident response.

Evidence: Training records, refresher schedules, and role-based certifications.

21. 21.

Requirement: Policies must govern secure storage, movement, and disposal of sensitive materials or equipment.

Evidence: Policy documents, tracking logs, and disposal approvals.

22. 22.

Requirement: Emergency and evacuation plans must balance safety and security and comply with legal standards.

Evidence: Evacuation procedures, floor plans, and compliance checklists.

23. 23.

Requirement: Procedures must govern asset movement, repair, and disposal, including monitoring and verification steps.

Evidence: Movement forms, repair logs, and security sign-offs.

24. 24.

Requirement: Audits must be conducted regularly to evaluate physical security controls and include corrective action tracking.

Evidence: Audit reports, CAPA trackers, and management review notes.

25. 25.

Requirement: Physical security must be embedded into business continuity and disaster recovery plans.

Evidence: BCP and DRP documents referencing physical security dependencies.

26. 26.

Requirement: Continuous improvement practices must apply to physical security systems via incident reviews, upgrades, and training updates.

Evidence: CAPA logs, upgrade plans, and training session evaluations.

27. 27.

Requirement: Stakeholder engagement processes must inform policy development and security improvement.

Evidence: Stakeholder meeting notes, feedback reports, and action logs.