MPS 16 – Technical Systems

Category: Protection

Tags: technical systems, risk management, redundancy, availability, cybersecurity, data protection, preventive maintenance, obsolescence management, data analytics, ISO 27001, Industry 4.0

Description: Minimum Performance Standard for Technical Systems. Defines the intent, required actions, and guidance for ensuring security-critical technical systems are risk-rated, fit for purpose, resilient, continuously available, and proactively managed. Promotes technology-led controls, strong internal data governance, structured preventive maintenance, and integration of automated monitoring and analytics. Aligned with ISO 27001 and Industry 4.0 standards for cybersecurity and infrastructure resilience.

Assessment Criteria (Structured)

1. 1.

Requirement: A documented Security Philosophy must prioritise technology-first design, redundancy, and human support roles.

Evidence: Signed philosophy outlining core principles and security architecture.

2. 2.

Requirement: An approved Technical Systems Policy must define risk-based design, performance standards, and data protection requirements.

Evidence: Policy document, risk matrix, and alignment checks against security objectives.

3. 3.

Requirement: Risk assessments must identify critical technical assets and required response protocols.

Evidence: Risk assessment reports and threat modelling outputs.

4. 4.

Requirement: A risk register must track ratings, repair times, and stakeholder feedback.

Evidence: Central risk register with update history and assignment tracking.

5. 5.

Requirement: Redundancy strategies must be documented for power, networks, and environment.

Evidence: Strategy documents, continuity test logs, and resilience KPIs.

6. 6.

Requirement: Live monitoring systems must provide automated alerts for system degradation or failure.

Evidence: Monitoring system screenshots and alert history logs.

7. 7.

Requirement: Automated workflows and escalation rules must be defined for incident handling.

Evidence: Workflow documentation, escalation paths, and role-based assignments.

8. 8.

Requirement: Preventive maintenance schedules must be documented and compliance tracked.

Evidence: Maintenance calendars, technician logs, and compliance dashboards.

9. 9.

Requirement: Data analytics systems must be in place to track availability, failures, and root causes.

Evidence: Dashboards, repair analytics, and reporting logs.

10. 10.

Requirement: Obsolescence management must include audits, risk analysis, spares strategy, and supplier alignment.

Evidence: Lifecycle tracking spreadsheets and critical component roadmaps.

11. 11.

Requirement: Procurement specifications must embed performance, resilience, and cybersecurity requirements.

Evidence: Spec sheets, procurement templates, and contract inclusions.

12. 12.

Requirement: Inventory management must reflect asset conditions, obsolescence status, and maintenance history.

Evidence: Inventory database, tag records, and update history.

13. 13.

Requirement: Disaster recovery plans must cover backups, automated shutdowns, and offsite storage.

Evidence: DRP documentation and test schedules.

14. 14.

Requirement: Role-based access must control all technical systems and log all activity.

Evidence: Access matrix, user logs, and password policy documentation.

15. 15.

Requirement: Monitoring logs must record incidents, alerts, and responses for all systems.

Evidence: Log extracts, mitigation records, and audit trails.

16. 16.

Requirement: System designs must support encryption, MFA, and secure data transfer and storage.

Evidence: Architecture diagrams and technical controls documentation.

17. 17.

Requirement: Surveillance and access data must be retained internally with defined access controls.

Evidence: Data protection policy, hosting configurations, and vendor restriction guidelines.

18. 18.

Requirement: Environmental controls must ensure safe operating ranges for all hardware.

Evidence: Sensor logs, temperature tracking, and UPS/failover proofing.

19. 19.

Requirement: Policies must cover patching, upgrades, version control, and environment separation (IT/OT).

Evidence: Change control forms, patching reports, and test environments.

20. 20.

Requirement: Vendor and supplier records must include SLAs, contacts, and support coverage.

Evidence: Supplier contracts, escalation paths, and SLA dashboards.

21. 21.

Requirement: An incident management system must document technical failures and associated corrective actions.

Evidence: IMS entries, RCA reports, and CAPA logs.

22. 22.

Requirement: Clear desk and screen policies must be implemented and enforced.

Evidence: Inspection reports, violation records, and awareness posters.

23. 23.

Requirement: Technical system audits must include redundancy validation, backup tests, and failure simulations.

Evidence: Audit reports and test logs.

24. 24.

Requirement: Management reviews must evaluate performance, availability, and downtime trends.

Evidence: Meeting minutes, trend reports, and improvement actions.