

## MPS 21 – Documentation and Metrics

**\*\*Category:\*\*** Proof It Works

**\*\*Tags:\*\*** documentation, document control, operational metrics, version control, audit readiness, assurance, performance reporting, recordkeeping, compliance, SOPs

**\*\*Description:\*\*** Minimum Performance Standard for Documentation and Metrics. Defines the intent, required actions, and guidance for managing records, procedures, and operational data to ensure audit readiness, version control, compliance, and data-driven assurance reviews. Supports the structured control and meaningful design of documentation and metrics to promote accountability, visibility, and continuous improvement across the security function.

### Assessment Criteria (Structured)

1. 1.

**\*\*Requirement:\*\*** A formal document control policy and process must exist covering version control, access, retention, and disposal.

**\*\*Evidence:\*\*** Approved document control policy and workflow logs.

2. 2.

**\*\*Requirement:\*\*** Document versioning and metadata tracking must be in place for all key security documentation.

**\*\*Evidence:\*\*** Version history, metadata fields, and document management system outputs.

3. 3.

**\*\*Requirement:\*\*** Core security documentation must be available, current, and accessible.

**\*\*Evidence:\*\*** Documents including security policies, strategies, SOPs, and technical system specifications.

4. 4.

**\*\*Requirement:\*\*** Security documentation must include site-specific plans and technical maintenance records.

**\*\*Evidence:\*\*** Site security plans and maintenance logs.

5. 5.

**\*\*Requirement:\*\*** A metrics framework must define KPIs aligned with security objectives and risk frameworks.

**\*\*Evidence:\*\*** KPI lists, mapping to objectives, and stakeholder review notes.

6. 6.

**\*\*Requirement:\*\*** Performance dashboards and statistical reports must be compiled and reviewed periodically.

**\*\*Evidence:\*\*** Dashboards, review logs, and report dissemination records.

7. 7.

**\*\*Requirement:\*\*** Technical system performance must be measured through defined metrics.

**\*\*Evidence:\*\*** System uptime logs, failure rates, maintenance history, and lifecycle trackers.

8. 8.

**\*\*Requirement:\*\*** Security metrics must be reviewed by management and used for improvement actions.

**\*\*Evidence:\*\*** Meeting records, CAPA logs, and performance reviews.

9. 9.

**\*\*Requirement:\*\*** Metrics and reports must comply with ISO, legal, and internal standards.

**\*\*Evidence:\*\*** Compliance checklists and audit references.

10. 10.

**\*\*Requirement:\*\*** Metrics and documentation must be archived securely and remain accessible for audit.

**\*\*Evidence:\*\*** Document archives, metadata logs, and access control systems.