MPS 13 – Engagement and Communication

Category: People and Culture

Tags: communication, employee engagement, security culture, incident reporting, leadership accountability, stakeholder engagement, people and culture

Description: Minimum Performance Standard for Stakeholder Engagement and Effective Communication. Defines the intent, required actions, and guidance for fostering a security-aware culture by engaging all personnel, promoting transparent reporting, building trust, and supporting collaborative risk management. Emphasises clear, two-way communication channels, employee engagement, leadership accountability, and partnerships with external stakeholders to reduce risks and protect organisational assets.

Assessment Criteria (Structured)

1. 1.

Requirement: An approved Employee Engagement and Security Communication Plan must define objectives and two-way channels between employees and security.

Evidence: Signed plan documents with outlined roles, processes, and continuous improvement goals.

2. 2.

Requirement: Security awareness content must be included in all employee induction processes.

Evidence: Induction materials, presentation decks, and employee confirmation records.

3. 3.

Requirement: Training materials must be documented and promote ethical behaviour and asset protection.

Evidence: Training slide decks, content summaries, and delivery records.

4. 4.

Requirement: Systems must be available for reporting security incidents, with options for confidentiality or anonymity.

Evidence: Incident reporting tools, access logs, and communication of reporting options.

5. 5.

Requirement: A formal investigation process must include root cause analysis and provide feedback to reporters.

Evidence: Investigation records, RCA templates, and responder feedback logs.

6. 6.

Requirement: Security incidents must be tracked, reported, and reviewed for trends.

Evidence: Incident logs, trend dashboards, and periodic reporting records.

7. 7.

Requirement: Employee engagement surveys must be conducted regularly to assess culture and communication effectiveness.

Evidence: Survey instruments, response summaries, and action plans.

8. 8.

Requirement: Leadership and management accountability must be defined and communicated.

Evidence: Policy documents, responsibility matrices, and briefings.

9. 9.

Requirement: Managers must be briefed on security responsibilities including asset management and escalation procedures.

Evidence: Briefing attendance records and agenda notes.

10. 10.

Requirement: Consultative processes must involve staff in identifying, assessing, and managing security risks.

Evidence: Meeting records, participation logs, and follow-up actions.

11. 11.

Requirement: Security teams must provide support to departments in control implementation and local planning.

Evidence: Advisory notes, planning templates, and engagement logs.

12. 12.

Requirement: New managers must receive induction training or briefings on security accountability.

Evidence: Manager training modules and training sign-off forms.

13. 13.

Requirement: Security messages must be reinforced through workplace signage and communication tools.

Evidence: Posters, digital signage plans, and photo documentation.

14. 14.

Requirement: Signage policies must define placement, design standards, and language clarity.

Evidence: Formal policy document with visuals and layout guidance.

15. 15.

Requirement: External stakeholder engagement strategies must be documented and linked to defined objectives.

Evidence: Engagement plans, stakeholder mapping, and strategy summaries.

16. 16.

Requirement: Formal partnerships or MOUs with external agencies must be documented and specify cooperative protocols.

Evidence: Signed MOUs, cooperation plans, and joint communication procedures.