8. Domains and Topics

TPN reviewed v4.10 Security Domains, Security Areas, and Security Topics. For v5.0, we updated the Security Domains to better reflect the intended objectives of the Best Practices and Implementation Guidance and to support the addition of Application and Cloud Security. See table below, sorted in alphabetical order.

Security Domains v4.10	Security Domains v5.0
Digital Security	Operational Security
Management Systems	Organization Security
Physical Security	Physical Security
	Technical Security

During review, TPN deemed the Security Area layer as unnecessary, and it was removed.

Security Areas v4.10
Asset Management
Content Management
Content Transfer
Facility
Infrastructure
Organization and Management
Transport

The v4.10 Security Topics numbered 47 in total and were overly complicated. We streamlined the v5.0 Security Topics to 12 which greatly simplifies the assessment process.

Security Topics v4.10	Security Topics v5.0
Account Management	Access Control
Alarms	Asset Management
Authentication	Cryptography
Authorization	Incident Management
Background Checks	Information Systems
Blank Media/Raw Stock Tracking	Logistics
Business Continuity & Disaster Recovery	Monitoring
Cameras	Network Security
Change Control & Configuration Management	Personnel Security
Client Assets	Policies & Procedures
Client Portal	Risk Management
Confidentiality Agreement	Vulnerability Management
Content Tracking	
Disposals	

Electronic Access Control
Entry/Exit Points
Executive Security Awareness/Oversight
Firewall/WAN/Perimeter Security
I/O Device Security
Identification
Incident Response
Internet
Inventory Counts
Inventory Tracking
Keys
Labeling
LAN/Internal Network
Logging and Monitoring
Mobile Security
Packaging
Perimeter Security
Policies and Procedures
Receiving
Risk Management
Searches
Security Organization
Security Techniques
Segregation of Duties
Shipping
System Security
Third Party Use & Screenings
Transfer Device Methodology
Transfer Systems
Transport Vehicles
Visitor Entry/Exit
Wireless
Workflow

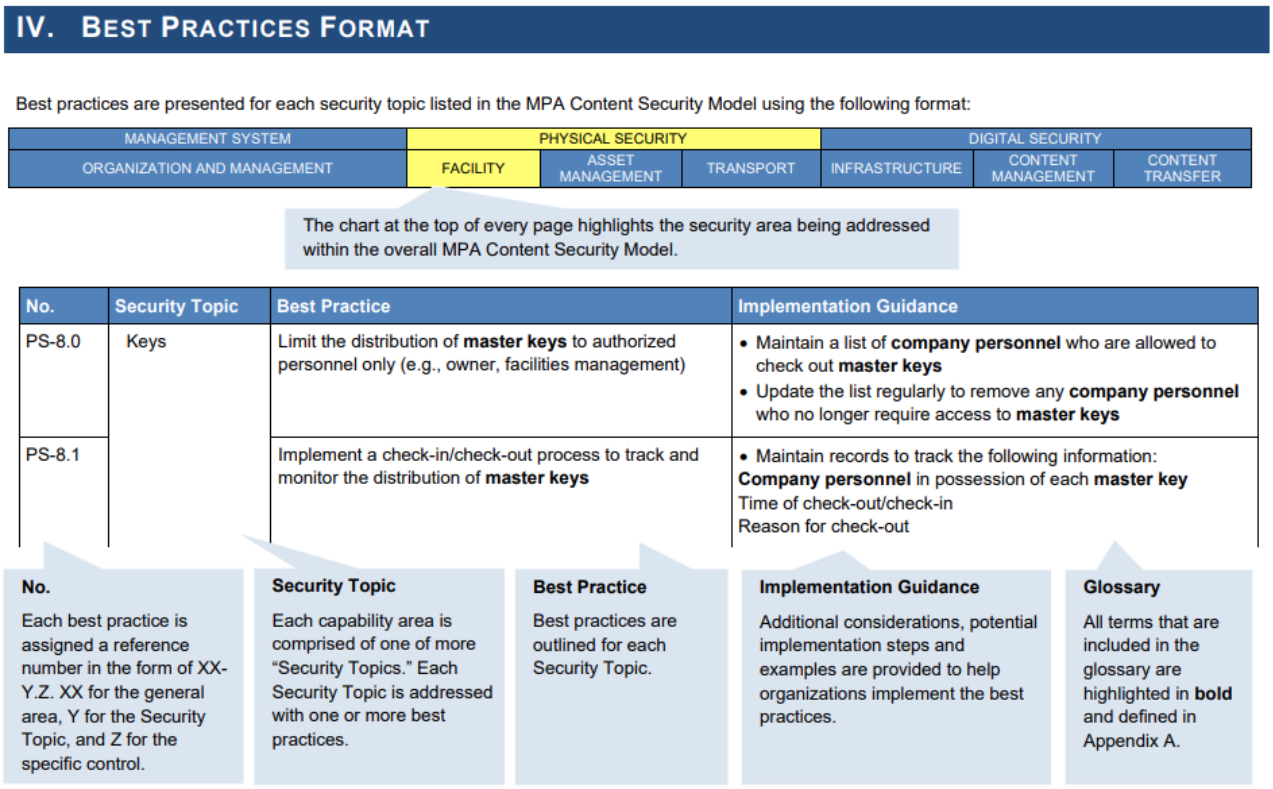
9. Glossary

As the scope of the MPA Content Security Best Practices v5.0 expanded to include Application and Cloud and the evolution of industry terms and technology continues, the Glossary was updated accordingly. The Glossary now contains key terms commonly used in the Media and Entertainment and Information Security industries related to Operational, Organizational, Physical, and Technical Security.

10. Functional Format

The MPA Site Best Practices and Common Guidelines v4.10 were published in a PDF format. The 105 pages were difficult to sort, filter, and incorporate into Service Provider's Standard Operating Procedures (SOPs). The updated MPA Best Practices v5.0 is published in an Excel format. When downloaded, this enables the user to sort, filter, and incorporate into the Service Provider's SOPs if needed.

MPA Site Best Practices and Common Guidelines v4.10



IV. BEST PRACTICES FORMAT

Best practices are presented for each security topic listed in the MPA Content Security Model using the following format:

MANAGEMENT SYSTEM	PHYSICAL SECURITY			DIGITAL SECURITY		
ORGANIZATION AND MANAGEMENT	FACILITY	ASSET MANAGEMENT	TRANSPORT	INFRASTRUCTURE	CONTENT MANAGEMENT	CONTENT TRANSFER

The chart at the top of every page highlights the security area being addressed within the overall MPA Content Security Model.

No.	Security Topic	Best Practice	Implementation Guidance
PS-8.0	Keys	Limit the distribution of **master keys** to authorized personnel only (e.g., owner, facilities management)	• Maintain a list of **company personnel** who are allowed to check out **master keys** • Update the list regularly to remove any **company personnel** who no longer require access to **master keys**
PS-8.1		Implement a check-in/check-out process to track and monitor the distribution of **master keys**	• Maintain records to track the following information: **Company personnel** in possession of each **master key** Time of check-out/check-in Reason for check-out

No.
Each best practice is assigned a reference number in the form of XX-Y.Z. XX for the general area, Y for the Security Topic, and Z for the specific control.

Security Topic
Each capability area is comprised of one of more "Security Topics." Each Security Topic is addressed with one or more best practices.

Best Practice
Best practices are outlined for each Security Topic.

Implementation Guidance
Additional considerations, potential implementation steps and examples are provided to help organizations implement the best practices.

Glossary
All terms that are included in the glossary are highlighted in **bold** and defined in Appendix A.

MPA Content Security Best Practices v5.0

Control No.	Domain	Topic	Best Practices: Minimum requirements where all components need to be fully implemented in order to be compliant with the overall Best Practice.	Implementation Guidance: Supplemental recommendations for Best Practices implementation. These are not requirements.	Site	Cloud	AICPA TSC 2017	CSA CCM v4.0.3	ISO 27002-2022	NIST 500-53 Rev. 5
OR-1	Organizational Security	Policies & Procedures	Establish, regularly review, and update upon key changes, the **Information Security Management System (ISMS)**, which is approved by leadership of the organization, which includes the following: • Control framework • **Governance, Risk and Compliance (GRC)**	Recommend implementing the following: • Reference established Information and Content Security frameworks e.g. MPA Best Practices, ISO27001's, NIST 800-53, SANS, CoBIT, CSA, CIS, etc. • Establish an independent team for Information Security, including a governance committee, to develop policies addressing threats, incidents, risks, etc. • Prepare organization charts and job descriptions to facilitate the designation of roles and responsibilities as it pertains to security	√	√	CC5.3	GRC-01 GRC-02	5.1 5.37	PM-1
OR-2	Organizational Security	Risk Management	Establish a formal, documented security risk management program, to include the following: • Address workflows, assets, and operations • Apply principles of **Confidentiality, Integrity, and Availability (CIA)** • Regularly review and upon key changes • Conduct a **risk assessment** annually • Document decisions on risk management, to include monitoring and reporting remediation status with relevant stakeholders	Recommend implementing the following: • Define a clear scope for the security risk assessment and modify as necessary • Incorporate a systematic approach that uses likelihood of risk occurrence, impact to business objectives/content protection and asset classification for assigning priority (e.g. **Business Impact Assessment (BIA)**) • Risks identified should tie into the business continuity and disaster recovery plans • Include risks to cloud environments and infrastructure if applicable • Conduct meetings with management and key stakeholders regularly to identify and document risks • A formal **exception policy** • Document and maintain a **Threat Modeling and Analysis** process as applicable • Ensure WFH/remote access content workflow risks are also documented and addressed as applicable • Leverage NISTIR 8286, FAIR frameworks, or ISO 3100:2018 • See NIST's **Secure Software Development Framework (SSDF)** NIST 800-218 (https://csrc.nist.gov/Projects/ssdf) as an example for Threat Modeling and on how to develop a **Secure Software Development Lifecyle (SSDLC)** process for coverage of training, requirements	√	√	CC1.3 CC3.1 CC3.2 CC4.1 CC5.1	CEK-07 GRC-02	5.8 5.21 7.5	CA-1 PM-10 PM-9 PM-29 RA-1

CONTINUOUS FEEDBACK PROCESS

TPN captured all stakeholder feedback and will continue to review and consider these comments for future updates. Additionally, we will monitor, review, and analyze progress made by the industry on the MPA Content Security Best Practices v5.0.

We look forward to working with the community on an ongoing basis for future enhancements. In the spirit of our collective forward momentum, collaboration, and innovation, the MPA Content Security Best Practices are now based on a solid foundation that will provide the industry with its most comprehensive roadmap for continuously addressing Content Security.