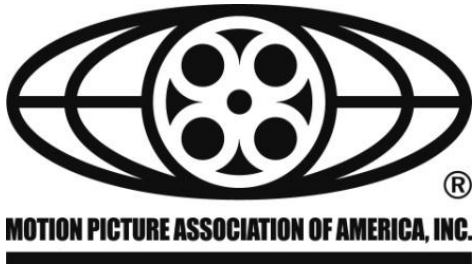

MPAA Site Security Program

CONTENT SECURITY BEST PRACTICES

POST-PRODUCTION SUPPLEMENTAL

Version 2.0

May 15, 2011

DOCUMENT HISTORY

Version	Date	Description	Author
1.0	December 31, 2009	Initial Public Release	Deloitte & Touche LLP MPAA MPAA Member Companies
2.0	May 15, 2011	Updates and Revisions Consolidation into Common Guidelines and Supplementals	PwC LLP MPAA MPAA Member Companies

I. POST-PRODUCTION OVERVIEW

General Description

Post Production facilities are responsible for many services such as digitization of content, sound and video editing, color correction and grading, quality control and digital mastering.

Facility

The following table describes the attributes of the content generally held at this facility type:

Type of Content
☐ Stills
☐ Script
☑ Audio Only
☑ Video and Audio

Video Attribute	Description
Completeness	☑ Full ☑ Partial
Resolution	☑ High ☐ Low
Quality	☑ Clean ☐ Watermarked ☐ Spoiled

Typical Risks

Typical security and content protection risks for this facility type include, but are not limited to, the following:

- Loss, interception, or theft of sensitive content such as:
  - Finishing, clean, high resolution content
  - Master audio files
  - Complete musical score
- Outsourcing to other third party facilities and individuals that the studios have no visibility into
- Weak physical access controls
- Unrestricted outbound Internet access on media transfer systems and devices
- Lack of network segregation that allows unauthorized access to content
- Facilities with limited resources that may discourage or limit the ability to implement security controls such as:
  - Physical security at entry and exit points
  - Chain of custody
  - Segregation of duties
  - Other advanced security controls

II. BEST PRACTICE SUPPLEMENTAL GUIDELINES

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

No.	Security Topic	Best Practice	Implementation Guidance
MS.S-1.0	Executive Security Awareness / Oversight	Establish an information security management system that implements a control framework (e.g., IS0 27001) for information security which is approved by executive management / owner(s)	
MS.S-3.0	Security Organization	Establish a security team that is responsible for proactively monitoring **information systems** and physical security to identify and respond to any suspicious activity	• Monitor **information systems** regularly throughout the day to detect possible incidents • Incorporate the **incident response** process to handle detected incidents • Consider implementing automatic notification to the team when suspicious activity involving **information systems** is detected • Implement a periodic review process to monitor the effectiveness of monitoring processes

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

No.	Security Topic	Best Practice	Implementation Guidance
MS.S-12.0	Content Security and Piracy Awareness	Provide in-depth training specific to the content handled by the facility	• Include security training on risks surrounding the transport and handling of content • Emphasize the individual responsibilities of each job function to protect content and mitigate piracy issues • Integrate training material to include the MPAA "Report Piracy" website and studio/client contact information • Provide internal anonymous telephone number and/or website to report piracy
MS.S-13.0	Third Party Use and Screening	Communicate to clients the use of third-party storage providers for physical assets	• Provide clients with due diligence reports for third party storage companies • Require clients to approve and sign-off on the use of third party storage companies
MS.S-13.3		Review access to third-party content delivery systems and websites annually	• Implement procedures to evaluate user access, such as: – Terminated users – Authorization levels – E-mail account validation

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

No.	Security Topic	Best Practice	Implementation Guidance
PS.S-4.1	Perimeter Security	Lock perimeter gates at all times and dedicate an on-site employee to handle remote unlocking capabilities	• Assign the front desk personnel the responsibility of managing visitor requests for entry • Place cameras at perimeter gates to verify visitor identity
PS.S-10.1	Cameras	Designate an employee or group of employees to monitor surveillance footage during operating hours and immediately investigate detected security incidents	• Incorporate the incident response process for handling detected security incidents

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

No.	Security Topic	Best Practice	Implementation Guidance
PS.S-13.0	Inventory Tracking	Use automated notification for assets that have been out of the **vault** for extended periods of time	• Establish expected check-out durations for each type of asset • Configure the content **asset management** system to automatically notify **vault** personnel when assets have not been returned within the expected timeframe

APPENDIX A — MAPPING OF SUPPLEMENTAL CONTROLS TO REFERENCES

The following table provides a general mapping of the best practices to the ISO 27001/27002 and NIST 800-53 standards. These standards can be referenced for further information on the implementation of the provided security controls.

No.	Security Topic	ISO 27002 Reference	NIST Reference
MS.S-1.0	Executive Security Awareness / Oversight	6.1.1, 6.1.2	PM-1, PM-2
MS.S-3.0	Security Organization	6.1.3	PE-6, PM-2, SI-4
MS.S-12.0	Content Security and Piracy Awareness	8.2.2	AT-3, CP-3
MS.S-13.0	Third Party Use and Screening	6.2.1	
MS.S-13.3		6.2.3, 8.3.3, 10.2, 11.2.4	AC-2, PS-4, PS-5, PS-7, SA-9
PS.S-4.1	Perimeter Security	9.1.1	PE-3
PS.S-10.1	Cameras	6.1.3, 9.1.1	IR-5, IR-6, PE-3, PE-6
PS.S-13.0	Inventory Tracking		SI-5

End of Document