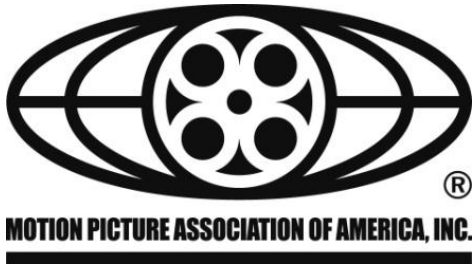

MPAA Site Security Program

CONTENT SECURITY BEST PRACTICES

CREATIVE ADVERTISING 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. Creative Advertising Overview

General Description

Creative Advertising facilities are responsible for developing, managing and handling advertising for titles owned by studios.

Facility

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

Type of Content
☑ Stills
☐ Script
☐ Audio (without video)
☑ 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:
  - Completed trailers, teasers, and other advertising products
  - Partial high quality video married with audio
  - High resolution stills and clips
  - Video, audio, and graphics far in advance of content release
- Weak security controls around workflow and asset management
- Lack of sophistication around IT networks and restriction of access to content
- Engagement of other small third party facilities and individuals that the studios have no visibility into
- Lack of security controls at smaller facilities that have limited resources, 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-13.3	Third Party Use and Screening	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-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-13.3	Third Party Use and Screening	6.2.3, 8.3.3, 10.2, 11.2.4	AC-2, PS-4, PS-5, PS-7, SA-9
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