MOTION PICTURE ASSOCIATION OF AMERICA, INC.

MPAA Site Security Program

CONTENT SECURITY BEST PRACTICES

DIGITAL SERVICES 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. Digital Services Overview

General Description

Digital Services facilities are responsible for the Digital Intermediate (DI) process, which involves film scanning, color adjustments and film recording. The DI process typically begins with film scanning, in which film is scanned into a digital format that can be manipulated and processed using computers. Tools can be used to perform edits such as color correction, dust busting, transitions, graphics, and final mastering with much greater precision and speed.

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:
  - Audio and video content on film, tape, hard drives and digital files
  - Full feature content in high quality and resolution
  - Digital masters
  - Film distribution masters
- Ad-hoc processes around asset management of content on film as well as on digital files that may not be consistently followed
- Use of external courier and delivery services for the transportation of full feature content
- Large amounts and various formats of highly sensitive content that requires high levels of security

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-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

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

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

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
PS.S-14.1	Inventory Counts	Monitor film elements (e.g., negatives, unprocessed film) constantly throughout the **workflow** process	• Reconcile film materials with work orders as they move through the **workflow** process • Track the movement of film materials using a chain of custody form
PS.S-16.0	Client Assets	Require two **company personnel** with separate access cards to unlock highly sensitive areas (e.g., safe, high-security cage) after-hours	

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-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
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
PS.S-16.0	Client Assets	10.1.3	AC-5

End of Document