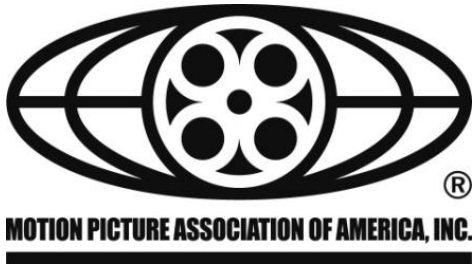

MPAA Site Security Program

CONTENT SECURITY BEST PRACTICES

DIGITAL CINEMA 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 Cinema Overview

General Description

Digital Cinema facilities are responsible for the digital mastering process and for the replication and distribution of full feature digital content to Digital Cinema theatres. These services can be performed together at a single facility or independently at separate facilities.

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:
  - Digital Source Masters (DSMs)
  - Digital Cinema Distribution Masters (DCDMs)
  - Digital Cinema Packages (DCPs)
  - Complete, clean, high resolution audio and video
- Ad-hoc processes around key generation and key management that may not be consistently followed at mastering houses
- Trusted Device Lists (TDLs) that are not updated to limit content playback to specified devices
- Replication and distribution of hard drives containing full feature DCPs that may be easily stolen during storage or transport
- Managing where drives are sent and returned

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-12.1		Provide training on the applications and processes surrounding **encryption** and **key management** for all individuals who handle encrypted content	• Include security training on the generation, distribution, and revocation of encryption keys as necessary for each individual's roles and responsibilities
MS.S-13.2	Third Party Use and Screening	Re-assess transportation and packaging vendors annually and when the vendor changes its location and/or provides additional services	• Implement procedures to track which vendors have undergone **due diligence** for the year (e.g., database repository, certificates of completion)

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-7.0	Authorization	Review access to restricted areas (e.g., **vault**, safe) on a monthly basis and when the roles or employment status of any **company personnel** and/or **third party workers** change	• Validate the status of **company personnel** and **third party workers** • Verify that access remains appropriate for each users' associated job function
PS.S-8.0	Electronic Access	Establish separate rooms for replication and for mastering	• Limit access to each room to personnel who require access for their job role • Enforce a **segregation of duties** model which restricts any single person from having access to both rooms

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
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	
PS.S-18.4	Disposals	Prohibit the use of third party companies for the destruction of DCDM drives or pre-released content	• Implement and develop procedures for the data destruction of DCDM drives or other physical **media** that contain pre-released content

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
DS.S-9.0	Logging and Monitoring	Implement logging mechanisms on all systems used for: • Key generation • **Key management** • Vendor certificate management	• Ensure that all generated keys and added certificates are traceable to a unique user

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
DS.S-10.0	Security Techniques	Implement a process for **key management** that addresses the following: • Approval and revocation of trusted devices • Generation, renewal, and revocation of content keys • Internal and external distribution of content keys	• Refine and document the **key management** process as necessary • Incorporate the **key management** process into the content **workflow** and identify risks at each stage of the **key management** lifecycle (i.e., generation, distribution, revocation)
DS.S-10.1		Confirm that devices on the **Trusted Devices List (TDL)** are appropriate based on rights owners' approval	• Require clients to provide a list of devices that are trusted for content playback • Only create Key Delivery Messages (KDMs) for devices on the **TDL**
DS.S-10.2		Confirm the validity of content keys and ensure that expiration dates conform with client instructions	• Require clients to provide expiration dates for content keys • Specify an end date for when keys expire to limit the amount of time for which content can be viewed

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-12.1		8.2.2, 12.3.1, 12.3.2	AT-3, SC-12
MS.S-13.2	Third Party Use and Screening	6.2.3, 10.2.2	PS-3

No.	Security Topic	ISO 27002 Reference	NIST Reference
PS.S-7.0	Authorization	9.1.2, 11.2.4	PE-2, PE-3, PE-6
PS.S-8.0	Electronic Access	9.1.2	PE-2, PE-3
PS.S-13.0	Inventory Tracking		SI-5
PS.S-16.0	Client Assets	10.1.3	AC-5
PS.S-18.4	Disposals	6.2.1	
DS.S-9.0	Logging and Monitoring	10.10, 12.3.1, 12.3.2	AU-1, AU-2, AU-3, AU-6, SC-12, SC-13
DS.S-10.0	Security Techniques	12.3.1, 12.3.2	SC-12, SC-13
DS.S-10.2		12.3.1, 12.3.2	SC-12, SC-13

End of Document