



**MPAA Site Security Program**

# **CONTENT SECURITY BEST PRACTICES**

## **FILM LAB**

## **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. FILM LAB OVERVIEW

## General Description

Film Labs are responsible for the development, processing, and editing of physical film. For productions that are shot on physical film and do not choose to go through the digital intermediate process, all processing and edits must be made using the physical film itself.

## Facility

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

Type of Content	
<input type="checkbox"/> Stills	
<input type="checkbox"/> Script	
<input type="checkbox"/> Audio Only	
<input checked="" type="checkbox"/> Video and Audio	
Video Attribute	Description
Completeness	<input checked="" type="checkbox"/> Full <input type="checkbox"/> Partial
Resolution	<input checked="" type="checkbox"/> High <input type="checkbox"/> Low
Quality	<input checked="" type="checkbox"/> Clean <input type="checkbox"/> Watermarked <input type="checkbox"/> 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:
  - Complete high quality audio and video
  - Release prints
- Recording of partial or full feature content during quality control reviews
- Lack of implementation and enforcement of policies prohibiting the use of digital recording devices
- Ad-hoc processes around the storage and destruction of scrap that may not be consistently followed
- Inadequate processes around shipping and receiving of film reels

## 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 <b>information systems</b> and physical security to identify and respond to any suspicious activity	<ul style="list-style-type: none"> <li>• Monitor <b>information systems</b> regularly throughout the day to detect possible incidents</li> <li>• Incorporate the <b>incident response</b> process to handle detected incidents</li> <li>• Consider implementing automatic notification to the team when suspicious activity involving <b>information systems</b> is detected</li> <li>• Implement a periodic review process to monitor the effectiveness of monitoring processes</li> </ul>

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-11.0	Disciplinary Measures	Include a provision in the disciplinary policy stating that a lack of cooperation with the exit search procedure can lead to disciplinary actions	<ul style="list-style-type: none"> <li>Identify appropriate disciplinary measures that are aligned with the severity and business impact of any security-related breaches caused by the individual</li> <li>Involve senior management in determining the actions to be applied</li> <li>Communicate potential sanctions to all <b>company personnel</b> and <b>third party workers</b></li> <li>Document the measures in the company handbook, security policies and other areas</li> <li>Communicate disciplinary measures in new hire orientation training</li> </ul>
MS.S-12.0	Content Security and Piracy Awareness	Provide in-depth training specific to the content handled by the facility	<ul style="list-style-type: none"> <li>Include security training on risks surrounding the transport and handling of content</li> <li>Emphasize the individual responsibilities of each job function to protect content and mitigate piracy issues</li> <li>Integrate training material to include the MPAA "Report Piracy" website and studio/client contact information</li> <li>Provide internal anonymous telephone number and/or website to report piracy</li> </ul>
MS.S-13.0	Third Party Use and Screening	Communicate to clients the use of third-party storage providers for physical assets	<ul style="list-style-type: none"> <li>Provide clients with <b>due diligence</b> reports for third party storage companies</li> <li>Require clients to approve and sign-off on the use of third party storage companies</li> </ul>
MS.S-13.1		Require international (to/from U.S.) transportation companies to be "Customs-Trade Partnership Against Terrorism" (CTPAT) certified	<ul style="list-style-type: none"> <li>Require international transportation companies to present proof of CTPAT certification upon first hire</li> <li>Maintain a list of CTPAT certified transportation companies</li> </ul>

No.	Security Topic	Best Practice	Implementation Guidance
MS.S-13.2		Re-assess transportation and packaging vendors annually and when the vendor changes its location and/or provides additional services	<ul style="list-style-type: none"> <li>• Implement procedures to track which vendors have undergone <b>due diligence</b> for the year (e.g., database repository, certificates of completion)</li> </ul>
MS.S-13.4		Incorporate security <b>due diligence</b> activities (e.g., security assessment, self-assessment questionnaire) as part of a selection and hiring process for third party workers who handle sensitive content	<ul style="list-style-type: none"> <li>• Consider the following:                             <ul style="list-style-type: none"> <li>- Require <b>third party workers</b> to provide their policies and procedures for handling content</li> <li>- Conduct interviews with the third party's management and key process owners to identify content handling procedures / controls for processing, storing and transmitting sensitive content</li> <li>- Request the third party to provide security <b>risk assessment</b> results and relevant remediation plans</li> </ul> </li> </ul>

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-1.0	Entry/Exit Points	Post security guards at all non-emergency entry/exit points	<ul style="list-style-type: none"> <li>Require security guards to visually inspect all individuals leaving the facility</li> <li>Implement a process by which guards report and investigate suspicious behavior</li> </ul>
PS.S-1.1		Lock and install alarms on all loading dock doors, and monitor loading dock doors while in use	<ul style="list-style-type: none"> <li>Unlock loading docks only for transactions that have a valid work order</li> <li>Require the appropriate <b>company personnel</b> to be present at all times during loading</li> </ul>
PS.S-1.2		Segregate the truck driver's entrance to prevent truck drivers from entering other areas of the facility	
PS.S-1.3		Implement a daily security patrol process with a randomized schedule and document patrolling results in a log	<ul style="list-style-type: none"> <li>Require security guards to patrol both interior and exterior areas</li> <li>Include a review of emergency exits, including verification of seals</li> <li>Consider using a guard tour patrol system to track patrolling (e.g., Checkpoint) and verify locks</li> </ul>
PS.S-1.4		Document, investigate, and resolve all incidents detected during security guard shifts	<ul style="list-style-type: none"> <li>Establish guidelines for triggering the <b>incident response</b> process</li> <li>Incorporate <b>incident response</b> procedures for handling detected security events</li> </ul>
PS.S-4.0		Perimeter Security	Install additional perimeter safeguards (e.g., fences, vehicle barricades) to decrease the risk of unauthorized access onto the premises

No.	Security Topic	Best Practice	Implementation Guidance
PS.S-4.1		Lock perimeter gates at all times and dedicate an on-site employee to handle remote unlocking capabilities	<ul style="list-style-type: none"> <li>• Assign the front desk personnel the responsibility of managing visitor requests for entry</li> <li>• Place cameras at perimeter gates to verify visitor identity</li> </ul>
PS.S-4.2		Station a security guard at perimeter entrances and implement a process (e.g., electronic gate arm, parking permits) to allow vehicles into the facility campus	<ul style="list-style-type: none"> <li>• Implement an electronic arm, that is manned by security personnel, to control vehicle access into the facility</li> <li>• Distribute parking permits to <b>company personnel</b> and <b>third party workers</b> who have completed proper paperwork</li> <li>• Require visitor vehicles to present identification and ensure that all visitors have been pre-authorized to enter the premises</li> </ul>
PS.S-7.0	Authorization	Review access to restricted areas (e.g., <b>vault</b> , safe) on a monthly basis and when the roles or employment status of any <b>company personnel</b> and/or <b>third party workers</b> change	<ul style="list-style-type: none"> <li>• Validate the status of <b>company personnel</b> and <b>third party workers</b></li> <li>• Verify that access remains appropriate for each users' associated job function</li> </ul>



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 <b>vault</b> for extended periods of time	<ul style="list-style-type: none"> <li>• Establish expected check-out durations for each type of asset</li> <li>• Configure the content asset management system to automatically notify <b>vault</b> personnel when assets have not been returned within the expected timeframe</li> </ul>
PS.S-14.0	Inventory Counts	Perform a weekly inventory count of each client's pre-release project(s), reconcile against asset management records, and immediately communicate variances to clients	<ul style="list-style-type: none"> <li>• Document all inventory counts</li> <li>• Do not allow <b>vault</b> staff to perform inventory counts (i.e., <b>segregation of duties</b>)</li> </ul>
PS.S-14.1		Monitor film elements (e.g., negatives, unprocessed film) constantly throughout the <b>workflow</b> process	<ul style="list-style-type: none"> <li>• Reconcile film materials with work orders as they move through the <b>workflow</b> process</li> <li>• Track the movement of film materials using a chain of custody form</li> </ul>

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-19.0	Shipping	Document and retain a separate log for truck driver information	<ul style="list-style-type: none"> <li>• Maintain a log of all truck drivers and include the following information:                             <ul style="list-style-type: none"> <li>- Name</li> <li>- License tags for the tractor and trailer</li> <li>- Affiliated company</li> <li>- Time and date of pick up</li> <li>- Content handled</li> </ul> </li> </ul>
PS.S-19.1		Require personnel picking up package(s) to verify the count against shipping document and obtain a signature from the shipping point	<ul style="list-style-type: none"> <li>• Require recipients to reconcile that the shipped count matches their work orders</li> <li>• Report back any discrepancies or damage to shipped goods immediately</li> </ul>
PS.S-19.3		Implement a formal process to record, monitor, and review travel times, routes, and delivery times for shipments between facilities	<ul style="list-style-type: none"> <li>• Establish a baseline for delivery times between common shipping points and monitor actual times for variance</li> <li>• Investigate, report, and escalate major variances to appropriate personnel</li> <li>• Designate approved rest stops</li> </ul>
PS.S-19.4		Do not allow film elements to leave the facility other than through shipping, except with a signed authorization pass	<ul style="list-style-type: none"> <li>• Create a form for documenting outbound assets that are transported via uncommon methods</li> <li>• Require authorization from appropriate personnel before assets can be carried out</li> <li>• Record any elements that leave the facility, whether through shipping or other means</li> </ul>
PS.S-19.5		Ship prints for pre-theatrical screenings in segments (e.g., odd versus even reels)	

No.	Security Topic	Best Practice	Implementation Guidance
PS.S-22.0	Packaging	Apply shrink wrapping to all shipments, and inspect packaging before final shipment to ensure that it is adequately wrapped	<ul style="list-style-type: none"> <li>• Apply shrink wrapping to individual assets (e.g., skids, pallets) or per spindle if bulk shipments are performed</li> </ul>
PS.S-23.0	Transport Vehicles	Include the following security features in transportation vehicles (e.g., trailers): <ul style="list-style-type: none"> <li>• Segregation from driver cabin</li> <li>• Ability to lock and seal cargo area doors</li> <li>• GPS for high-security shipments</li> </ul>	<ul style="list-style-type: none"> <li>• Use vehicles equipped with GPS or XDA tracking systems for delivery of sensitive content and high-value assets</li> </ul>

## 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
<b>MS.S-3.0</b>	Security Organization	6.1.3	PE-6, PM-2, SI-4
<b>MS.S-11.0</b>	Disciplinary Measures	5.1.1, 8.2.2, 8.2.3	AT-2, PS-8
<b>MS.S-12.0</b>	Content Security and Piracy Awareness	8.2.2	AT-3, CP-3
<b>MS.S-13.0</b>	Third Party Use and Screening	6.2.1	
<b>MS.S-13.2</b>		6.2.3, 10.2.2	PS-3
<b>MS.S-13.4</b>		6.2.3, 8.1.2, 10.2	PS-3
<b>PS.S-1.1</b>		9.1.6	PE-3, PE-7, PE-16
<b>PS.S-1.2</b>		9.1.2, 9.1.6	PE-3, PE-7, PE-16
<b>PS.S-1.3</b>			PE-1

No.	Security Topic	ISO 27002 Reference	NIST Reference
<b>PS.S-1.4</b>		13.1.1, 13.1.2	IR-1
<b>PS.S-4.0</b>	Perimeter	9.1.1	PE-3
<b>PS.S-4.1</b>	Security	9.1.1	PE-3
<b>PS.S-4.2</b>		9.1.1	PE-3
<b>PS.S-7.0</b>	Authorization	9.1.2, 11.2.4	PE-2, PE-3, PE-6
<b>PS.S-13.0</b>	Inventory Tracking		SI-5
<b>PS.S-14.0</b>	Inventory Counts	7.1.1	CM-8
<b>PS.S-19.0</b>	Shipping	10.8.2, 10.8.3	MP-5, SA-9
<b>PS.S-19.1</b>		10.8.2, 10.8.3	
<b>PS.S-19.3</b>		10.8.2	MP-5, PE-16
<b>PS.S-19.4</b>		10.8.3	PE-16
<b>PS.S-22.0</b>		Packaging	10.8.3

**End of Document**