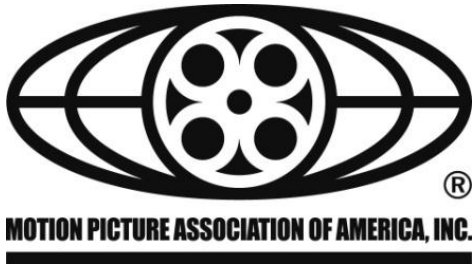

MPAA Site Security Program

CONTENT SECURITY BEST PRACTICES

IFE AND HOSPITALITY 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. IFE and Hospitality Services Overview

General Description

In-Flight Entertainment (IFE) and Hospitality facilities are responsible for the distribution of feature content used for playback on airplanes and other non-theatrical sites (such as hotels, cruise ships, ferries, libraries, hospitals and prisons). These facilities perform several processes, including the review of screeners, the encoding and encryption of content, and the integration of content with the IFE software and console.

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:
  - Complete audio and video on hard drives
  - High quality partial or full feature content
  - IFE masters
- Smaller airlines and non-theatrical sites that have little or no security around the storage of content
- Ad-hoc processes around the following areas:
  - Notification of losses and theft of missing screeners
  - Asset management of content

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

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-3.0	Security Organization	6.1.3	PE-6, PM-2, SI-4
PS.S-13.0	Inventory Tracking		SI-5

End of Document