MOTION PICTURE ASSOCIATION OF AMERICA, INC.

MPAA Site Security Program

CONTENT SECURITY BEST PRACTICES

VISUAL EFFECTS (VFX) 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. Visual Effects (VFX) Overview

General Description

Visual Effects facilities are responsible for augmenting live action shots with visual effects, including digital animation, computer generated imager, and other forms of special effects.

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:
  - High resolution content
  - Spoilers for digital sets, backgrounds, character looks, key plot lines, and latest designs for costumes or graphics
  - Digital effects and computer generated animations
- Leakage of raw footage without visual effects that may impact reputation and overall revenue of a title
- Lack of security controls around artist workstations that may allow outbound transfer of content
- Employee disclosure of sensitive project information via word of mouth, personal websites or social media

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
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

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
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

End of Document