



MPAA Global Site Security Program

CONTENT SECURITY BEST PRACTICES

In-Flight Entertainment and Hospitality Services

Version 1.0
December 31, 2009

Document History

Version	Date	Description	Author
1.0	12/31/2009	Initial public release	Deloitte & Touche LLP MPAA MPAA Member Companies

In cooperation with

Deloitte.

Table of Contents

I – BEST PRACTICES OVERVIEW	4
Introduction	4
Purpose and Applicability	4
Additional Best Practices Available	6
Questions or Comments	6
Document Layout and Organization	7
Information Security Management System (ISMS)	8
Format of Best Practices	9
2 – BEST PRACTICE GUIDELINES	10
Control Environment	10
Organization and Management – Organization Maturity	10
Organization and Management – Policies and Procedures	11
Organization and Management – Incident Response	12
Organization and Management – Process Management	13
Competency – Recruitment and Personnel	14
Competency – Training and Education	16
Competency – Vendor Management	17
Physical Security	18
Facility – Facility Access	18
Facility – Facility Security	21
Facility – Facility Authorization	24
Facility – Facility Monitoring	27
Asset Management – Inventory and Asset Management	31
Asset Management – Physical Asset Security	33
Transport – Shipping and Receiving	36
Transport – Package and Transport	37
Digital Security	38
Infrastructure – Infrastructure Security	38
Infrastructure – System Security	40
Infrastructure – Infrastructure Authentication and Authorization	41
Infrastructure – Infrastructure Monitoring	42
Content Management – Content Authorization	43
Content Management – Content Security	45
Content Management – Content Tracking	46
Content Transfer – Content Transfer Security	47
Content Transfer – Content Transfer Authorization	49
Content Transfer – Content Transfer Tracking	50
APPENDIX A – GLOSSARY	51
APPENDIX B – FREQUENTLY ASKED QUESTIONS	53
APPENDIX C – SUGGESTED POLICIES AND PROCEDURES	54
APPENDIX D – BIBLIOGRAPHY	56
APPENDIX E – MPAA 24-HOUR TIP LINE	57

I – BEST PRACTICES OVERVIEW

Introduction

The Motion Picture Association of America, Inc. (“MPAA”) has a 30-year history of managing site security surveys on behalf of its Member Companies: Walt Disney Studios Motion Pictures, Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corporation, Universal City Studios LLLP, and Warner Bros. Entertainment Inc. In 2007, the MPAA engaged Deloitte & Touche LLP (“Deloitte & Touche”) to perform global site security surveys using a standardized survey model, process, and report. Since then, almost 200 facilities providing a wide-variety of services within the motion picture and television value chain (production, post-production, distribution, etc.) have been surveyed globally.

The MPAA is committed to protecting the rights of those who create entertainment content for audiences around the world. From creative arts to the software industry, more and more people around the globe make their living based on the power of their ideas. This means there is a growing global stake in protecting intellectual property rights and recognizing that these safeguards are a cornerstone of a healthy global information economy.

The MPAA Global Site Security Program’s purpose is to ensure that Member Company content is protected during production, post-production, marketing, and distribution. This is accomplished by:

- Assessing and evaluating content security at third-party outside vendors;
- Reinforcing the importance of securing Member Company content; and
- Providing a standard survey vehicle for further individual discussions regarding content security between Member Companies and their business partners.

Purpose and Applicability

The main objective of this document is to provide current and future vendors engaged by Member Companies with an understanding of general content security expectations and current industry best practices. Decisions regarding the use of vendor(s) by any particular Member Company are made by each Member Company solely on a unilateral basis.

Content security best practices are designed to take into consideration the services a facility provides, the type of content the facility generally handles, and in what release window the facility operates.

This document applies directly to In-Flight Entertainment and Hospitality Services. Assumptions are based on the type of content generally handled and the typical window in which content is released.

IFE/HOSPITALITY SERVICES		
FACILITY SERVICES	TYPE OF CONTENT	RELEASE WINDOW
<ul style="list-style-type: none"> Laboratory Services (Encoding, Applying Encryption) Content Integration Services Content Loading End-User Interface (Devices, Interfaces) Hotel, Airline and Cruise Ship Tape/Drive Duplication and Distribution 	High-Resolution – Full or Partial Content	Pre-Home Entertainment Catalog

Please note that best practices outlined in this document are subject to local, state, and federal laws or regulations.

Please also note that best practices outlined in this document, as well as the industry standards or ISO references contained herein, are subject to change periodically.

Compliance with best practices is strictly voluntary. This is not an accreditation program.

Additional Best Practices Available

Best practices presented in this document are part of a set of ten best practices created based on different facility types. The following table shows a listing of all best practices published:

FACILITY SERVICE TYPE	TYPICAL FACILITY SERVICES
Audio, Dubbing, and Sub-Titling	Original and Foreign Language Dubbing, Subtitling, SFX, Scoring, ADR/Foley
Creative Advertising	Non-Finishing, Trailer, TV Spots, Teasers, Graphics
Digital Services	Digital Intermediate, Scanning, Film Recording
Distribution	Distribution, Fulfillment
DVD Creation	Compression, Authoring, Encoding, Regionalization, Special Features, Checkdisc QC
Film Lab	Negative Processing, Cutting, Release Prints
IFE/Hospitality Services	IFE Lab, IFE Integration, Hotel, Airline, and Cruise Ship Distribution
Post-Production Services (Small)	Telecine, Duplication, Editing, Audio, Finishing, QC, VFX
Post-Production Services (Large)	Telecine, Duplication, Editing, Audio, Finishing, QC, VFX
Replication	Pre-Mastering, Mastering, Replication, Checkdisc Creation

Questions or Comments

If you have any questions or comments about the best practices, please email: sitesurvey@mpaa.org.

Document Layout and Organization

These best practices are organized according to the MPAA Content Security Maturity Model, which is used as the basis for all site security surveys worldwide. The MPAA Content Security Maturity Model provides an analytic framework for assessing a facility's capabilities to secure content. It is comprised of 25 dimensions across three areas: (1) control environment, (2) physical security, and (3) digital security.

The components of the MPAA Content Security Maturity Model are drawn from relevant ISO standards (27001/27002), security standards (i.e., NIST), and industry best practices. The relevant security references are also included in the guidelines.

Information Security Management System (ISMS)

The control environment best practices are listed first for a reason – physical or digital security controls are only effective if there is an appropriate understanding of risk by management; monitoring and enforcement of company policies; and communication to employees, freelancers/temps, and vendors alike.

The importance of the control environment is highlighted in the ISO 27001 standard through the definition of an Information Security Management System (ISMS). The standard provides detail on the creation of an effective ISMS, including topics on the overall system, management responsibility, internal audits, management review, improvement, and others.

Throughout the document, ISO 27002 is also referenced. This refers to selected topics that would likely be applicable to the respective facility service and applied in accordance with the statement of applicability (SOA) defined by the ISMS. Which controls are relevant and/or address the risks present in an environment should be driven by the ISMS. Exceptions are any issues of legal compliance and continuity.

With a strong ISMS in place, an organization can work with others to identify risks and improve security within individual facilities and throughout the industry.

Format of Best Practices

Best practices are presented for each of the 25 capability dimensions in a table such as the one shown below. Each table includes a capability dimension description that summarizes relevant topics for that dimension, followed by the best practices for each topic. Additional considerations are noted in the next column, followed by links to specific references in other security standards (e.g., ISO 27001). The example below looks at the “Facility Monitoring” capability dimension under the “Facility” capability area.

FACILITY		FACILITY MONITORING	
Description	A CCTV system is implemented to monitor the facility. Processes are implemented to review CCTV footage and keycard access logs. CCTV footage and keycard access logs are retained based on Company’s log retention/rotation policy. Searches are performed on individuals, packages, and vehicles (e.g., review of trunks) when applicable.		
Topics	Best Practices	Additional Considerations	Reference
Cameras	<ul style="list-style-type: none"> Install a CCTV system that covers areas where content is stored or processed 	<ul style="list-style-type: none"> Cameras in dark areas should accommodate for light conditions (e.g., low-light or infrared camera in machine room) 	ISO 27001: A.10.10.2 NIST 800-53/PE-6

Each capability dimension is comprised of one or more “Topics.”

Best practices are outlined for each topic. They are listed in an additive manner and are not exclusive.

If applicable, additional considerations for implementation will also be listed per topic. These considerations provide additional details to aid in the implementation of best practices.

Best practices have been mapped to ISO standards 27001 and 27002, as well as to NIST 800-53. Please refer to Appendix D for other guides.

2 – BEST PRACTICE GUIDELINES

Control Environment

The following best practices correspond to the control environment area of the MPAA Content Security Maturity Model. These best practices are intended for the implementation of security policies, procedures, and controls for the handling of client assets.

ORGANIZATION AND MANAGEMENT		ORGANIZATION MATURITY	
Description	Controls implemented by executive management that enable the organization to identify security threats, develop formal action plans, establish roles and responsibilities, and budget for the implementation of security controls.		
Topics	Best Practices	Additional Considerations	Reference
Risk Assessment	<ul style="list-style-type: none"> Perform a formal, documented evaluation of content security risks in workflows and update annually Identify areas for security improvements, prioritize, and implement controls to address risk 	<ul style="list-style-type: none"> Documentation of risks identified and remediation efforts should be maintained Key risks should reflect where the facility believes content losses may occur (e.g., risk of content leaving the facility) 	ISO 27001: A.14.1.2 ISO 27002: 4.1-4.2 ISO 27005 NIST 800-53 CA-2, RA-2, 3, 4
Security Organization	<ul style="list-style-type: none"> Identify security key point(s) of contact and formally define roles and responsibilities 	<ul style="list-style-type: none"> None 	ISO 27001: A.6.1.2 ISO 27002: 6.1, 8.1.1 NIST 800-53 PS-2, PL-2
Budgeting	<ul style="list-style-type: none"> Plan and budget for security initiatives, upgrades, and maintenance 	<ul style="list-style-type: none"> None 	NIST 800-53 SA-2

ORGANIZATION AND MANAGEMENT		POLICIES AND PROCEDURES	
Description	Formal policies, procedures, and guidelines implemented in order to minimize the possibility of inappropriate handling of assets and execution of implemented controls.		
Topics	Best Practices	Additional Considerations	Reference
Policies and Procedures	<ul style="list-style-type: none"> Establish policies and procedures regarding asset and content security; policies can be documented as part of the employee handbook 	<ul style="list-style-type: none"> The employee handbook should be made available to all employees and include the following topics: <ul style="list-style-type: none"> Human resources policies Asset handling policies Digital recording devices (e.g., ipod, camera phone) IT system security policy (e.g., password, unique user) <p>Please see Appendix C for the complete list of policies and procedures to consider</p>	<p>ISO 27001: A.5.1</p> <p>ISO 27002: 5.1</p> <p>NIST 800-53 PL-1</p>

ORGANIZATION AND MANAGEMENT		INCIDENT RESPONSE	
Description	The process and established procedures that are followed by the organization in order to respond to and minimize the impact of an incident, as well as procedures to report to appropriate stakeholders.		
Topics	Best Practices	Additional Considerations	Reference
Incident Response	<ul style="list-style-type: none"> Define an incident response and escalation procedure Incidents should be recorded, investigated, resolved, and communicated to clients 	<ul style="list-style-type: none"> Also consider leveraging the MPAA tips hotline for anonymous tips on suspicious activity – please refer to the 24-hour tip hotline contact information in Appendix E A tip website is also available and located at: http://www.mpa.org/ReportPiracy/ReportPiracy.aspx 	<p>ISO 27001: A.13.2.1</p> <p>ISO 27002: 13.1</p> <p>NIST 800-53 IR-1,2,3,5,6</p>

ORGANIZATION AND MANAGEMENT		PROCESS MANAGEMENT	
Description	A workflow is implemented by the Company, including checkpoints and segregation of duties. The workflow is monitored to ensure controls remain operating as implemented.		
Topics	Best Practices	Additional Considerations	Reference
Workflow	<ul style="list-style-type: none"> Implement a formal workflow (i.e., supported by email or a work order system) that includes tracking of assets and authorization checkpoints throughout the production process 	<ul style="list-style-type: none"> Workflow diagrams (e.g., Visio diagrams) can be used to facilitate the implementation of a formal workflow 	<p>ISO 27002: 10.1</p> <p>NIST 800-53 AC-4, AU-6</p>
Segregation of Duties	<ul style="list-style-type: none"> Segregate duties across the workflow (e.g., role-based, per job function) considering the following (among others): <ul style="list-style-type: none"> Vault and machine room personnel Shipping/receiving (department or dedicated resource) and duplication/content loading personnel Asset movement within the facility (e.g., runners) separate from vault and/or production area 	<ul style="list-style-type: none"> Segregation of duties can be achieved by the implementation of manual controls (e.g., approval from supervisor before shipping devices), automated controls in the work ordering system (e.g., automated approval for each stage of the workflow), and physical access controls (e.g., restricting machine room and duplication area) For instances where duties cannot be segregated due to resource limitations, consider implementing monitoring controls to act as a check and balance 	<p>ISO 27001: A.11.2.4, A.10.1.3</p> <p>ISO 27002: 10.1.3</p> <p>NIST 800-53 AC-5, AU-6</p>

COMPETENCY		RECRUITMENT AND PERSONNEL	
Description	The process of recruiting personnel includes controls to mitigate the risk of hiring personnel that would pose a higher threat to client assets and/or digital content. Controls can be comprised of background checks, confidentiality agreements, and disciplinary measures.		
Topics	Best Practices	Additional Considerations	Reference
Background Checks	<ul style="list-style-type: none"> Perform professional reference and criminal background checks before hiring all personnel who have access to facilities that handle content Where background checks are not allowed by law, document as an exception and use reference checks 	<ul style="list-style-type: none"> Criminal background checks should include state and nation-wide records for positions with higher clearance; criminal background checks are subject to local laws and regulations Education, certification and/or credit checks should be performed when applicable 	ISO 27001: A.8.1.2 ISO 27002: 8.1.2
Confidentiality Agreements	<ul style="list-style-type: none"> Require all employees to sign confidentiality (non-disclosure) agreements upon hiring Remind employees that confidentiality applies after termination or leaving the Company Explain the importance of confidentiality/NDA in non-legal terms, as necessary 	<ul style="list-style-type: none"> Consider requiring all employees to re-sign the NDA on an annual basis 	ISO 27001: A.8.1.3 ISO 27002: 6.1.5, 8.1.3

COMPETENCY		RECRUITMENT AND PERSONNEL		
Description	The process of recruiting personnel includes controls to mitigate the risk of hiring personnel that would pose a higher threat to client assets and/or digital content. Controls can be comprised of background checks, confidentiality agreements, and disciplinary measures.			
Topics	Best Practices	Additional Considerations	Reference	
Disciplinary Measures	<ul style="list-style-type: none"> Define and communicate disciplinary measures for violations of Company policies to all employees 	<ul style="list-style-type: none"> Communication of disciplinary measures can be achieved in several forms, including employee handbook and new hire orientation 	ISO 27001: A.8.2.3 ISO 27002: 8.2.3	

COMPETENCY		TRAINING AND EDUCATION	
Description	Security and anti-piracy training and awareness programs established by the Company and given to all employees and temps upon hiring, as well as on a periodic basis.		
Topics	Best Practices	Additional Considerations	Reference
Security/ Piracy Awareness	<ul style="list-style-type: none"> • Provide piracy and security awareness training at least upon hire/on-boarding • Training should include an overview of content security handling policies 	<ul style="list-style-type: none"> • Additional security awareness communication can come in many forms, such as posters, periodic distribution of newsletters, or communication in management meetings • Also consider leveraging the MPAA tips hotline for anonymous tips on suspicious activity – please refer to the 24-hour tip hotline contact information in Appendix E • A tip website is also available and located at: http://www.mpa.org/ReportPiracy/ReportPiracy.aspx 	<p>ISO 27001: A.8.2.2</p> <p>ISO 27002: 8.2.2</p> <p>NIST 800-53 AT-2,3</p>

COMPETENCY		VENDOR MANAGEMENT	
Description	The organization follows a vendor screening process that ensures vendors emulate the organization's internal policies, procedures, and standards as they relate to the protection of client assets.		
Topics	Best Practices	Additional Considerations	Reference
Vendor Use and Screening	<ul style="list-style-type: none"> Require all vendors, freelancers, and temps handling content to sign confidentiality (non-disclosure) agreements upon hire Remind vendors that confidentiality applies after terminating relationships with the company Vendors used should be bonded where appropriate (e.g., courier service) Vendors should have restricted access to production areas, unless required for their job functions; vendors such as cleaning crews should not have access to sensitive areas (e.g., vault, integration workstations) If third-party vendors are used that significantly handle content, consider performing a security review prior to being engaged 	<ul style="list-style-type: none"> Consider implementing a probationary period (i.e., 90 days) for freelancers and/or temps before granting elevated security clearance (physical/digital) 	<p>ISO 27001: A.8.1.2</p> <p>ISO 27002: 6.2, 10.2</p>

Physical Security

The following best practices correspond to the physical security area of the MPAA Content Security Maturity Model. These best practices are intended for the securing of physical assets throughout the production process, from receiving assets to the delivery of finished product to clients.

FACILITY		FACILITY ACCESS	
Description	Access controls implemented at the facility in order to prevent unauthorized access, including physical entry protocols for employees and visitors, as well as means of identifying internal personnel, temps, and visitors.		
Topics	Best Practices	Additional Considerations	Reference
Entry/Exit Points	<ul style="list-style-type: none"> If the facility does not have a segregated, access-controlled area beyond reception, exterior doors should be locked at all times If the facility has a segregated access-controlled area beyond reception, exterior entrances may be unlocked during business hours 	<ul style="list-style-type: none"> If the facility is in design phase, we suggest that the reception area is completely segregated from the production facility (i.e. an access control door is used to positively identify personnel upon entry to the facility) 	ISO 27001: A.9.1.2 (Physical controls) ISO 27002: 9.1.2 NIST 800-53 PE-3,6

FACILITY		FACILITY ACCESS	
Description	Access controls implemented at the facility in order to prevent unauthorized access, including physical entry protocols for employees and visitors, as well as means of identifying internal personnel, temps, and visitors.		
Topics	Best Practices	Additional Considerations	Reference
Visitor Entry/Exit	<ul style="list-style-type: none"> • Implement a visitor protocol that includes the use of a visitors’ log and assigns means of identification to visitors (e.g., stickers, paper badges, plastic badges) • A detailed visitors’ log should be maintained for audit, including: <ul style="list-style-type: none"> – Name – Company – Purpose of the visit – Time-in/Time-out – Persons visited • If visitor badges function as a keycard, visitor badges must not grant access to production areas • All visitors should be escorted while on-site 	<ul style="list-style-type: none"> • If visitor badges are issued: <ul style="list-style-type: none"> – Visitor badges functioning as access keycards must not grant access to production areas – Badges should make visitors easily distinguishable from regular Company employees (e.g., color coded) • Do not allow visitors to view the names of previously registered visitors • Plastic visitor’s badges should be accounted for daily • Paper badges should be dated with visitor’s name 	<p>ISO 27001: A.9.1.2, A.9.1.6</p> <p>ISO 27002: 9.1.2</p> <p>NIST 800-53 PE-7</p>

FACILITY		FACILITY ACCESS	
Description	Access controls implemented at the facility in order to prevent unauthorized access, including physical entry protocols for employees and visitors, as well as means of identifying internal personnel, temps, and visitors.		
Topics	Best Practices	Additional Considerations	Reference
Identification	<ul style="list-style-type: none"> Provide employees, long-term vendors/freelancers, and service providers with an identification badge (preferably with a picture) that is required to be visible at all times Vendor/freelancer and service providers badges should be issued with a set expiration date based on an approved timeframe that is displayed on the badge 	<ul style="list-style-type: none"> Badges should make employees easily distinguishable from vendors/freelancers and service providers (e.g., color coded) Consider omitting company location and other specific information on the badge 	<p>ISO 27001: A.9.1.2</p> <p>NIST 800-53 PE-3</p>

FACILITY		FACILITY SECURITY	
Description	Security controls implemented at the facility in order to secure the perimeter, including the use of fences/walls, and alarm systems, as well as the implementation of emergency protocols to enable the Company to keep client assets secure.		
Topics	Best Practices	Additional Considerations	Reference
Perimeter Security	<ul style="list-style-type: none"> • Based on the location and layout of the facility, management should implement a strong perimeter security environment that may include a combination of the following: <ul style="list-style-type: none"> – Restricting perimeter access through the use of walls, fences, and/or gates that, at a minimum, are secured after hours; walls/fences should be 8 feet or higher – Securing and enclosing, as necessary, common external areas such as smoking areas and open balconies – Sufficient external camera coverage around common exterior areas (e.g., smoking areas), as well as parking (please refer to camera topic below) – Being cognizant of the overuse of company signage that could create targeting – Using alarms around the perimeter, as necessary 	<ul style="list-style-type: none"> • If the facility is shared with other businesses and is located on a separate floor(s) (by itself), consider using keycard access authentication in elevators to gain access to the floor(s) after hours • If visitors are uncommon at the facility, consider securing perimeter gates at all times and using remote unlocking/buzz-in capabilities 	ISO 27001: A.9.1.1 ISO 27002: 9.1.1 NIST 800-53 PE-3
Emergency	<ul style="list-style-type: none"> • Install a power backup system (e.g., Uninterruptible Power Supply “UPS”) to 	<ul style="list-style-type: none"> • If a UPS is not available, individual power supplies can be installed for each of the 	ISO 27001: A.9.2.2

FACILITY		FACILITY SECURITY	
Description	Security controls implemented at the facility in order to secure the perimeter, including the use of fences/walls, and alarm systems, as well as the implementation of emergency protocols to enable the Company to keep client assets secure.		
Topics	Best Practices	Additional Considerations	Reference
Protocol	<p>support security installations such as the CCTV system, alarm system, and keycard system (as applicable) for at least 15 minutes to allow enough time for the facility to be secured upon emergency (e.g., power outage)</p> <ul style="list-style-type: none"> Power backup should be tested on an annual basis 	<p>security systems in place (e.g., alarm, CCTV, and keycard system)</p> <ul style="list-style-type: none"> Keycard systems should be configured as fail-safe in case of a power outage (i.e., doors allow employees to exit but require positive authentication to enter) Consider including the security of content in the overall facility emergency plan 	<p>ISO 27002: 9.2.2</p> <p>NIST 800-53 PE-10, 11, CP-2,3,4</p>

FACILITY		FACILITY SECURITY	
Description	Security controls implemented at the facility in order to secure the perimeter, including the use of fences/walls, and alarm systems, as well as the implementation of emergency protocols to enable the Company to keep client assets secure.		
Topics	Best Practices	Additional Considerations	Reference
Alarms	<ul style="list-style-type: none"> • Install an alarm system that covers all entrances and exits • The alarm should be audible and provide escalation notification directly to company personnel in charge of security and/or be monitored by a central security group or third-party • Alarm should be consistently enabled when the facility is idle or has limited staff on-site (e.g., at night, holiday) 	<ul style="list-style-type: none"> • Assign unique alarm codes (to arm and disarm the alarm) to appropriate personnel only • Alarm codes are to be changed regularly at intervals defined by management (e.g., semi-annually) • After normal business hours, alarm system should cover storage areas and vaults (through motion sensors) to add an extra layer of security • Consider using multiple alarm zones 	<p>ISO 27002: 9.2</p> <p>NIST 800-53 PE-6, IR-2,3</p>

FACILITY		FACILITY AUTHORIZATION	
Description	Processes are implemented by the Company in order to allow physical access to the facility only if approved by appropriate parties, as well as implementation of access control mechanisms to restrict access within the facility.		
Topics	Best Practices	Additional Considerations	Reference
Authorization	<ul style="list-style-type: none"> No formal, documented authorization process is expected Remove keycard access rights and recall keys promptly upon termination Review access to sensitive areas (e.g., vault, machine room, edit bays) on a quarterly basis The periodic review process should validate the status of employees, temps, and contractors, as well as validate that access remains appropriate for the users' associated responsibility 	<ul style="list-style-type: none"> None 	<p>ISO 27001: A.11.2.1, A.11.2.4</p> <p>ISO 27002: 11.1., 11.2</p> <p>NIST 800-53 PE-1,2,3</p>

FACILITY		FACILITY AUTHORIZATION	
Description	Processes are implemented by the Company in order to allow physical access to the facility only if approved by appropriate parties, as well as implementation of access control mechanisms to restrict access within the facility.		
Topics	Best Practices	Additional Considerations	Reference
Electronic Access	<ul style="list-style-type: none"> • Implement keycard access or individual keypin (combination code) throughout the facility to cover selective areas where content is stored or processed – these are typically as follows: <ul style="list-style-type: none"> - Vault - Machine room - Duplication area - Content loading area - Testing areas - Shipping/receiving - Any area where assets can be copied or outputted • Edit bays that have output capability must also have access key cards or keypin (combination code) • Restrict keycard system administration to appropriate personnel • Blank keycards should be stored in a locked cabinet and remain disabled prior to being assigned to personnel • In case of a lost keycard, keycard should be disabled in the system before issuing a new keycard 	<ul style="list-style-type: none"> • None 	<p>ISO 27001: A.9.1.3</p> <p>ISO 27002: 9.1.2</p> <p>NIST 800-53 IA-4,5</p>

FACILITY		FACILITY AUTHORIZATION	
Description	Processes are implemented by the Company in order to allow physical access to the facility only if approved by appropriate parties, as well as implementation of access control mechanisms to restrict access within the facility.		
Topics	Best Practices	Additional Considerations	Reference
Master Keys	<ul style="list-style-type: none"> Limit master keys to authorized personnel only (e.g., owner, facilities management); use high security keys (i.e., can only be copied by specific locksmith) Remove physical locks for sensitive areas (e.g., vault, machine room) where keycard access control system is implemented Rooms should be dedicated to screening purposes and locked when not in use 	<ul style="list-style-type: none"> None 	NIST 800-53 IA-5

FACILITY		FACILITY MONITORING	
Description	A CCTV system is implemented to monitor the facility. Processes are implemented to review CCTV footage and keycard access logs. CCTV footage and keycard access logs are retained based on Company’s retention/rotation policy. Searches are performed on individuals, packages, and vehicles (e.g., review of trunks) when applicable.		
Topics	Best Practices	Additional Considerations	Reference
Cameras	<ul style="list-style-type: none"> • Install a CCTV system that records areas where content is stored or processed; this typically includes the following areas: <ul style="list-style-type: none"> – All entry/exit points – Shipping/receiving – Vault entry – Vault interior – Machine room – Duplication area – Content loading area – Any area where assets can be copied or outputted • Cameras in dark areas should accommodate for light conditions (e.g., low-light or infrared camera in machine room) • CCTV equipment (e.g., DVRs) should be stored in a secure location (e.g., computer room, locked closet, cage) with access control • Restrict logical access to the CCTV system to administrators only • Review camera positioning, image quality, and retention on an ad-hoc basis 	<ul style="list-style-type: none"> • Image quality should be adequate to positively identify individuals – typically at least 6 frames per second and at a resolution of 320 x 240 • Camera footage may be recorded on disk or tape; date and time burnt into the recorded video 	ISO 27001: A.10.10.2 NIST 800-53 PE-6

FACILITY		FACILITY MONITORING	
Description	A CCTV system is implemented to monitor the facility. Processes are implemented to review CCTV footage and keycard access logs. CCTV footage and keycard access logs are retained based on Company’s retention/rotation policy. Searches are performed on individuals, packages, and vehicles (e.g., review of trunks) when applicable.		
Topics	Best Practices	Additional Considerations	Reference
Camera and Keycard Retention	<ul style="list-style-type: none"> Retain CCTV footage and keycard access logs for at least 90 days in a secure location Restrict access to CCTV footage (Tapes/DVR) and keycard access logs to personnel responsible for physical security 	<ul style="list-style-type: none"> None 	ISO 27001: A.10.10.1 ISO 27002: 10.10 NIST 800-53 AU 9,11

FACILITY		FACILITY MONITORING	
Description	A CCTV system is implemented to monitor the facility. Processes are implemented to review CCTV footage and keycard access logs. CCTV footage and keycard access logs are retained based on Company’s retention/rotation policy. Searches are performed on individuals, packages, and vehicles (e.g., review of trunks) when applicable.		
Topics	Best Practices	Additional Considerations	Reference
Key card Logging and Monitoring	<ul style="list-style-type: none"> Review keycard access logs (e.g., failed access attempts, odd access times) to high security areas on an as needed basis and investigate all exceptions 	<ul style="list-style-type: none"> None 	ISO 27001: A.10.10.2 NIST 800-53 PE-8, AU 3,6

FACILITY		FACILITY MONITORING	
Description	A CCTV system is implemented to monitor the facility. Processes are implemented to review CCTV footage and keycard access logs. CCTV footage and keycard access logs are retained based on Company’s retention/rotation policy. Searches are performed on individuals, packages, and vehicles (e.g., review of trunks) when applicable.		
Topics	Best Practices	Additional Considerations	Reference
Searches	<ul style="list-style-type: none"> Consider including a statement in human resource policies that stipulate that bags/packages are subject to search 	<ul style="list-style-type: none"> None 	<ul style="list-style-type: none"> None

ASSET MANAGEMENT		INVENTORY AND ASSET MANAGEMENT	
Description	Inventory tracking is performed by a Media Asset Management System, inventory counts are performed on a periodic basis and blank media is tracked and counted periodically.		
Topics	Best Practices	Additional Considerations	Reference
Inventory Tracking	<ul style="list-style-type: none"> • Implement a media asset management system or inventory tracking database to provide detailed tracking of physical assets (client masters and newly created); asset management system should have the following capabilities: <ul style="list-style-type: none"> - Require individual user IDs with user authentication - Check-in and check-out - Tracking of individuals - Location (e.g., staging) - Time/date - Transaction log • Tag (e.g., sticker, barcode) client assets upon receipt, as well as created media (e.g., tapes, encrypted hard drives); screeners should also be tagged and tracked • Use studio AKAs (“alias”) when applicable in asset tracking system and on any physical assets 	<ul style="list-style-type: none"> • Dual barcode should be applied (asset and container/case) • Consider retaining asset movement transaction logs for at least 90 days 	<p>ISO 27001: A.7.1.1</p> <p>ISO 27002: 7.1</p> <p>NIST 800-53 MP-3, AU-6,11</p>

ASSET MANAGEMENT		INVENTORY AND ASSET MANAGEMENT	
Description	Inventory tracking is performed by a Media Asset Management System, inventory counts are performed on a periodic basis and blank media is tracked and counted periodically.		
Topics	Best Practices	Additional Considerations	Reference
Inventory Counts	<ul style="list-style-type: none"> Implement a daily aging report (manually or through the asset management system) to identify high value assets checked out from the vault and not checked back in; investigate all exceptions; this applies to masters as well as screeners received by clients Perform a quarterly physical inventory count of client assets (e.g., masters); investigate and resolve variances identified Ensure segregation of duties between vault personnel and employee(s) performing inventory counts 	<ul style="list-style-type: none"> As an alternative, consider performing cycle counts by client or asset type (e.g., Digi-beta tape), depending on how stored 	ISO 27001: A.7.1.1 ISO 27002: 7.1 NIST 800-53 IR-4,5
Blank Media/ Raw Stock Tracking	<ul style="list-style-type: none"> Barcode blank media tapes and hard drives upon receipt Inventory blank stock on a monthly basis Blank media should be checked out based on proper work order request and returned to the secure location or locked in the staging area at end of each shift 	<ul style="list-style-type: none"> None 	ISO 27001: A.10.7.1 ISO 27002: 7.1 NIST 800-53 MP-4,5, IR-4,5

ASSET MANAGEMENT		PHYSICAL ASSET SECURITY	
Description	Client assets, blank media/raw stock, and production systems are stored in secure locations with access restricted to appropriate personnel. In addition, scrap/disposal assets are stored in a secure location before destruction and all disposals/destructions are logged.		
Topics	Best Practices	Additional Considerations	Reference
Client Assets	<ul style="list-style-type: none"> Implement a safe in the vault to house high-value, pre-released client assets (e.g., screeners), as well as finished and WIP Store client assets and finished/WIP in secure locations (e.g., vault, secure staging area) when not being used Restrict access to client assets and secure location to appropriate personnel 	<ul style="list-style-type: none"> None 	ISO 27001: A.9.2.1 ISO 27002: 9.2.1 NIST 800-53 MP-2

ASSET MANAGEMENT		PHYSICAL ASSET SECURITY	
Description	Client assets, blank media/raw stock, and production systems are stored in secure locations with access restricted to appropriate personnel. In addition, scrap/disposal assets are stored in a secure location before destruction and all disposals/destructions are logged.		
Topics	Best Practices	Additional Considerations	Reference
Blank Media/Raw Stock	<ul style="list-style-type: none"> Store blank media (e.g., blank tapes) in a segregated area (e.g., locked cabinet, in the vault) with a custodian designated; blank media should not be stored in the machine room or other areas that have output capabilities 	<ul style="list-style-type: none"> A segregated blank media area must include access control mechanisms (e.g., traditional key or keycard) and must be restricted to the custodian(s) of blank media only 	<p>ISO 27001: A.9.2.1</p> <p>ISO 27002: 9.2.1</p> <p>NIST 800-53 MP-4</p>
Production Systems	<ul style="list-style-type: none"> Segregate access to the following production areas: <ul style="list-style-type: none"> Vault Machine room Server room (if separate from machine room) Edit bays Content loading stations Encryption stations Duplication areas Restrict the use of DVD burners to only secure areas Restrict access to production systems to appropriate personnel only 	<ul style="list-style-type: none"> Consider using diskless nodes for edit bays – hard drives are not located in edit bay/suite but in a secured location 	<p>ISO 27001: A.9.1.2</p> <p>ISO 27002: 9.1.2</p> <p>NIST 800-53 CM-5</p>

ASSET MANAGEMENT		PHYSICAL ASSET SECURITY	
Description	Client assets, blank media/raw stock, and production systems are stored in secure locations with access restricted to appropriate personnel. In addition, scrap/disposal assets are stored in a secure location before destruction and all disposals/destructions are logged.		
Topics	Best Practices	Additional Considerations	Reference
Disposals	<ul style="list-style-type: none"> Rejected and/or damaged stock should be accounted for and reconciled against inventory; they should be erased, degaussed, shredded, or physically destroyed before disposal Store elements targeted for scrap/disposal in a secure location/container and establish a process to prevent copying and reuse of assets prior to disposal (e.g., degaussing, DVD shredding, hard drive destruction); elements should be destroyed as soon as possible but at most within 30 days; all working physical and digital copies must be destroyed (content shredding) Hard drives scheduled to be reused should be wiped clean of content following U.S. Department of Defense standards Disposed assets must be noted as such in the asset management system; asset records should be marked as disposed but not deleted A certificate of destruction should be obtained if a third-party destruction company is used 	<ul style="list-style-type: none"> None 	<p>ISO 27001: A.10.7.2</p> <p>ISO 27002: 9.2.6, 10.7.2</p> <p>NIST 800-53 MP-6</p>

TRANSPORT		SHIPPING AND RECEIVING	
Description	Process to receive and ship assets in and out of the facility, including techniques used to track asset shipping and receiving details.		
Topics	Best Practices	Additional Considerations	Reference
Shipping	<ul style="list-style-type: none"> Track asset shipping details; shipping logs should include details of time of shipment, sender, recipient, and content Validate assets leaving the facility against a valid work/shipping order Retain shipping logs for at least 90 days Obtain recipient signature for all high-value asset shipments Log courier(s) and/or individual(s) picking up assets 	<ul style="list-style-type: none"> Door or window to shipping/receiving area should be locked when there are no shipping/receiving activities Couriers/delivery personnel should not be allowed in production areas of the facility 	ISO 27001: A.10.8. ISO 27002: 10.8.3 NIST 800-53 AU-6
Receiving	<ul style="list-style-type: none"> Inspect content upon receipt and compare to shipping documents (e.g., packing slip, bill of lading); any discrepancy should be reported to sender immediately Record identity of receiver and transporter including details of time asset was received, delivery entity, recipient, and content Barcode assets received and input into the asset management system Store assets in vault upon barcoding/receipt; if assets are received by receptionist, secure assets (e.g., safe, locked cabinet) prior to pick-up 	<ul style="list-style-type: none"> Couriers/delivery personnel should not be allowed in production areas of the facility 	ISO 27001: A.10.8.3 ISO 27002: 10.8.3 NIST 800-53 AU 6, MP-3,5

TRANSPORT		PACKAGE AND TRANSPORT	
Description	Controls implemented to prevent assets from being targeted during the shipping process, including techniques for labeling, packaging, and transportation of assets.		
Topics	Best Practices	Additional Considerations	Reference
Labeling	<ul style="list-style-type: none"> Do not include title information on packing labels 	<ul style="list-style-type: none"> Return address should be included Consider removing the name of the Company from shipping labels 	ISO 27001: A.10.8.3 ISO 27002: 10.8.3
Packaging	<ul style="list-style-type: none"> Ship all assets in closed/sealed containers (not open bags or tapes/DVDs by themselves); this applies to hand-carried as well as courier service 	<ul style="list-style-type: none"> None 	ISO 27001: A.10.8.3 ISO 27002: 10.8.3
Transport Vehicles	<ul style="list-style-type: none"> Not applicable for facility service 	<ul style="list-style-type: none"> Consider using vehicles with GPS tracking and XDA systems for delivery 	ISO 27001: A.10.8.3 ISO 27002: 10.8.3
Segmentation	<ul style="list-style-type: none"> Not applicable for facility service 	<ul style="list-style-type: none"> None 	ISO 27001: A.10.7.3

Digital Security

The following best practices correspond to the digital security area of the MPAA Content Security Maturity Model. These best practices are intended for the securing of digital assets throughout the production process, from the reception/ingestion of assets to the delivery of finished products to clients.

INFRASTRUCTURE		INFRASTRUCTURE SECURITY	
Description	Logical security controls implemented at the infrastructure or network layers of the production/content network. This includes network servers, routers, switches, and other network devices.		
Topic	Best Practices	Additional Considerations	Reference
LAN	<ul style="list-style-type: none"> Segment the production/content network from other networks. (e.g., office network) Apply MAC address security at the switch level to restrict non-production systems (e.g., laptops) from connecting to the production or content network Do not allow remote access to the production/content network 	<ul style="list-style-type: none"> Segmentation can be implemented by using one of the following methods: <ol style="list-style-type: none"> Physical separation (e.g., air-gap) Logical separation using virtual local area networks (VLAN) with an appropriate access control list(s) (ACL) applied on the applicable VLANs Logical separation using a firewall with appropriate access rule sets applied to restrict access to the production network from other network segments All unused switch ports on the production/content network should be disabled to avoid unauthorized connections Static IP addresses should be used and DHCP disabled on the production/content network 	ISO 27001: A.11.4.5 ISO 27002: 11.4.5 NIST 800-53 AC-17

INFRASTRUCTURE		INFRASTRUCTURE SECURITY	
Description	Logical security controls implemented at the infrastructure or network layers of the production/content network. This includes network servers, routers, switches, and other network devices.		
Topic	Best Practices	Additional Considerations	Reference
WAN	<ul style="list-style-type: none"> Segment WAN(s) by using firewalls and/or routers with an access control list (ACL) to prevent unauthorized access to the internal production/content network Prohibit access to the production/content network from public Internet 	<ul style="list-style-type: none"> Common network protocols should be restricted, such as Telnet and FTP 	ISO 27001: 11.4.7 ISO 27002: 11.4.7 NIST 800-53 SC-7
Internet	<ul style="list-style-type: none"> Prohibit Internet access on systems (desktops/ servers) that process or store digital content 	<ul style="list-style-type: none"> Consider also implementing appropriate filtering tools on the office network to prevent sending content through email or limit size of attachments Consider using a separate workstation or Citrix session to access the Internet for editing rooms; machines with internet access are to have all I/O ports disabled (USB, FireWire, SCSI) 	ISO 27001: A.11.4.6 ISO 27002: 11.4.6 NIST 800-53 AC-20
Wireless	<ul style="list-style-type: none"> Prohibit the use of wireless devices on the production network 	<ul style="list-style-type: none"> If wireless devices must be used on the production/content network for business requirements, ensure that appropriate security controls are put into place. (e.g., strong authentication, encryption protocol - avoid WEP, using MAC address filtering) 	ISO 27001: A.11.4.3 ISO 27002: 11.4.3 NIST 800-53 AC-18

INFRASTRUCTURE		SYSTEM SECURITY	
Description	The use of input/output devices has been blocked and/or is monitored on production systems where digital content is stored or processed. Anti-virus software is implemented to prevent production/content network from being infected with viruses and/or malicious code.		
Topic	Best Practices	Additional Considerations	Reference
I/O Device Security	<ul style="list-style-type: none"> Block input/output devices (e.g., USB, firewire, and SCSI ports) output capabilities based on a defined standard applied on all systems that handle or store digital content For stations used to load content, consider the use of I/O port monitoring software that would detect port usage Implement 128 bit encryption on all hard drives and USB devices used to transport content 	<ul style="list-style-type: none"> For Microsoft Windows-based systems – it is possible to change the registry setting to restrict write access to I/O devices For Mac based systems – you may remove the mass storage file to control write access on production stations 	ISO 27001: A.15.2.2 ISO 27002: 12.1
Anti-Virus	<ul style="list-style-type: none"> Scan file-based content for viruses prior to being digitized/ingested on a non-production workstation Install anti-virus software on all Windows-based systems (desktops/servers) that process or store digital content Update Windows anti-virus definitions at least on a daily basis 	<ul style="list-style-type: none"> If the production network is fully isolated from other networks, anti-virus software is generally not required on production systems; however, files should be scanned for viruses before being ingested or digitized Due to the infrequent nature of viruses, there is not an expectation that anti-virus software is present on Apple/Mac, Linux, and Unix-based machines 	ISO 27001: A.10.4.1 ISO 27002: 10.4

INFRASTRUCTURE		INFRASTRUCTURE AUTHENTICATION AND AUTHORIZATION	
Description	Authentication mechanisms have been implemented to restrict access to production/content network. Administration access rights are restricted to appropriate personnel in charge of production/content network security. This pertains to network devices, as well as the operating system on production workstations and servers.		
Topic	Best Practices	Additional Considerations	Reference
Admin- istration Rights	<ul style="list-style-type: none"> Assign system administration rights on network devices (e.g., servers, routers, switches, firewalls) and production system operating systems to personnel responsible for managing the network and production devices (typically IT/Network administrators) Implement unique administration credentials 	<ul style="list-style-type: none"> Administration rights should only be assigned to personnel responsible for network management activities with no responsibilities over the production processes Default system administration credentials should be renamed and its use restricted to special situations requiring such system privileges only (e.g., OS version update, installing patches) 	<p>ISO 27001: A.11.6.1, A.11.2.2, A.10.10.4</p> <p>ISO 27002: 11.2.2</p> <p>NIST 800-53 AC-3, AU-6</p>
Authent- ication	<ul style="list-style-type: none"> Enforce the use of unique usernames and passwords to access production systems/networks Enforce a strong password policy to gain access to the production/content network and network devices (e.g., firewalls, routers, switches) Implement password protected screen savers for key content servers and workstations (e.g., staging, content servers) to be enabled after 20 minutes of inactivity 	<ul style="list-style-type: none"> Password policies are subject to system constraints, however, consider: <ul style="list-style-type: none"> Minimum password length of 6 characters Using 3 of the following parameters: upper case, lower case, numbers, and special characters Maximum password age of 90 days Maximum invalid logon attempts defined between three and six tries 	<p>ISO 27001: A.11.6.1</p> <p>ISO 27002: 11.4</p> <p>NIST 800-53 IA-2, AC-3, 7</p>

INFRASTRUCTURE		INFRASTRUCTURE MONITORING	
Description	Processes used for the logging and monitoring of activities performed on the production/content network, including routers, switches, and other network devices. Also, includes processes to maintain logs for an appropriate period of time.		
Topic	Best Practices	Additional Considerations	Reference
Logging and Monitoring	<ul style="list-style-type: none"> • Enable basic logging on infrastructure devices in order to track and monitor the production/content network 	<ul style="list-style-type: none"> • Consider monitoring logs on an as needed basis to investigate any unusual activity • Logs should track successful and unsuccessful access attempts to the production/content network 	<p>ISO 27001: A.10.10.1</p> <p>ISO 27002: 10.10</p> <p>NIST 800-53 AU-3,6</p>
Log Retention	<ul style="list-style-type: none"> • Retain logs for at least 90 days • Restrict log access to appropriate personnel 	<ul style="list-style-type: none"> • A server can also be implemented to manage the logs in a central repository such as syslog server or Security Information Management (SIM) system. • Protect logs from unauthorized deletion or modification by applying appropriate access rights on log files 	<p>ISO 27001: A.10.10.1</p> <p>ISO 27002: 10.10</p> <p>NIST 800-53 AU-9,11</p>

CONTENT MANAGEMENT		CONTENT AUTHORIZATION	
Description	Process to manage user access rights to digital content, including the processes to manage access requests, access changes, and access terminations, as well as controls to limit administration rights. This pertains to content storage devices (e.g., SAN, NAS, and content server).		
Topics	Best Practices	Additional Considerations	Reference
Production Access Authorization	<ul style="list-style-type: none"> Implement a user access management process to manage access requests, access changes, and access terminations to the content storage devices (e.g., SAN, NAS, content server) Periodically review user access to content on an ad-hoc basis (e.g., after each project) 	<ul style="list-style-type: none"> Evidence of the user provisioning process can be maintained in several forms, including email The periodic review should focus on identifying any terminated employees/freelancers, as well as validating system permissions to handle content (e.g., read, write) 	<p>ISO 27001: A.11.2.1, A.11.2.4</p> <p>ISO 27002: 11.5, 11.6</p> <p>NIST 800-53 AC-13, AU-3</p>
User Access Rights	<ul style="list-style-type: none"> Apply user access rights to digital content on content storage devices (e.g., SAN, NAS, content server) using individual profiles based on minimum project requirements 	<ul style="list-style-type: none"> Consider segregation of duties - personnel responsible for assigning access to digital content should not be responsible for production activities 	<p>ISO 27001: A.11.2.2</p> <p>ISO 27002: 11.1.1, 11.2.1, 11.5.2</p> <p>NIST 800-53 AC-6, MP-2</p>

CONTENT MANAGEMENT		CONTENT AUTHORIZATION	
Description	Process to manage user access rights to digital content, including the processes to manage access requests, access changes, and access terminations, as well as controls to limit administration rights. This pertains to content storage devices (e.g., SAN, NAS, and content server).		
Topics	Best Practices	Additional Considerations	Reference
Admin- istration Rights	<ul style="list-style-type: none"> Assign administration rights to content storage devices (e.g., SAN, NAS, content server) to appropriate personnel (e.g., IT personnel) that have no responsibility over the production processes Enforce the use of unique usernames and passwords to content storage devices (e.g., SAN, NAS, content server) 	<ul style="list-style-type: none"> Default system administration credentials should be renamed and its use restricted to special situations requiring such system privileges only (e.g., SAN system update) 	ISO 27001: A.11.2.2 ISO 27002: 11.2.2 NIST 800-53 AC-3, IA-2

CONTENT MANAGEMENT		CONTENT SECURITY	
Description	Advanced security techniques are available to be used on all client assets, including watermarking, fingerprinting, and encryption.		
Topics	Best Practices	Additional Considerations	Reference
Advanced Security Techniques	<ul style="list-style-type: none"> Implement 128 bit encryption (e.g., Windows Media DRM) on all hard drives used for content distribution Limit access to encryption keys to authorized personnel 	<ul style="list-style-type: none"> Please work with your client to determine further advanced security requirements, such as visible or invisible watermarking We recommend that you please contact the client security team if you are receiving content that is higher grade than needed to perform functions 	<p>ISO 27001: A.15.1.2</p> <p>ISO 27002: 10.6.2, 12.3.1, 15.1.6</p> <p>NIST 800-53 MP-3</p>

CONTENT MANAGEMENT		CONTENT TRACKING	
Description	Activities performed with digital content (e.g., access, copy, movements) are tracked through the use of object audit logging and/or digital content management system. Also, audit logs are retained for an appropriate length of time. This pertains to content storage devices (e.g., SAN, NAS, and content server).		
Topics	Best Practices	Additional Considerations	Reference
Logging and Monitoring	<ul style="list-style-type: none"> Implement tracking mechanisms (e.g., object audit logging) to enable digital content tracking on content storage devices (e.g., SAN, NAS, content server) 	<ul style="list-style-type: none"> None 	ISO 27002: 10.10 NIST 800-53 MP-5, AU-6
Log Retention	<ul style="list-style-type: none"> Retain audit logs for at least 90 days Restrict audit log access to personnel in charge of storage device administration 	<ul style="list-style-type: none"> None 	ISO 27002: 10.10 NIST 800-53 AU-9,11

CONTENT TRANSFER		CONTENT TRANSFER SECURITY	
Description	Secure transfer tools are implemented and dedicated content transfer devices are used. If a web portal is used for sharing content with clients, it has to be restricted to authorized users and protected by appropriate security mechanisms.		
Topics	Best Practices	Additional Considerations	Reference
Transfer Tools	<ul style="list-style-type: none"> Implement the use of secure transfer tools that use 128-bit encryption as a minimum and strong authentication mechanisms Contact the client’s security team immediately if you are unable to send or receive content through secure channels 	<ul style="list-style-type: none"> Alternatives to FTP include Secure FTP, FTPS, and other common proprietary tools (e.g., Aspera, Digi-Delivery, WAM!NET, Signiant, and Smartjog, among others) 	<p>ISO 27001: A.10.8.4</p> <p>ISO 27002: 10.8, 10.9</p> <p>NIST 800-53 SC-8,9</p>
Transfer Device Methodology	<ul style="list-style-type: none"> Implement and use dedicated devices for content transfers (behind a firewall) Segment devices dedicated to transfer files from devices that store or process content Implement a workflow that restricts the transfer of files to designated personnel only 	<ul style="list-style-type: none"> Consider placing the dedicated content transfer devices in a DMZ Editing stations and content storage servers are not to be used to directly transfer content 	<p>R ISO 27001: A.10.8.4</p> <p>ISO 27002: 10.8, 10.9</p> <p>NIST 800-53 MP-5</p>

CONTENT TRANSFER		CONTENT TRANSFER SECURITY	
Description	Secure transfer tools are implemented and dedicated content transfer devices are used. If a web portal is used for sharing content with clients, it has to be restricted to authorized users and protected by appropriate security mechanisms.		
Topics	Best Practices	Additional Considerations	Reference
Client Portal	<ul style="list-style-type: none"> Not applicable for facility service 	<ul style="list-style-type: none"> None 	ISO 27001: A.11.4.2 ISO 27002: 10.8, 10.9, 11.6 NIST 800-53 AC-3, IA-2, SC-8,9

CONTENT TRANSFER		CONTENT TRANSFER AUTHORIZATION	
Description	Process to manage user access rights on content transfer tools, including the processes to request and grant access and assign system privileges, as well as controls to limit administration rights.		
Topics	Best Practices	Additional Considerations	Reference
User Access Rights	<ul style="list-style-type: none"> Restrict access rights on transfer tools based on job function Use unique credentials (e.g., username and password) to access transfer tools 	<ul style="list-style-type: none"> None 	ISO 27001: A.11.2.4, A.11.6.1 ISO 27002: 11.2, 11.5 NIST 800-53 AC-3,6, IA-2
Administration Rights	<ul style="list-style-type: none"> Assign transfer tool administration rights to appropriate personnel only Enforce the use of unique usernames and passwords for users with administration rights to manage transfer tools 	<ul style="list-style-type: none"> None 	ISO 27001: A.10.10.4, A.11.2.2 ISO 27002: 11.2.2 NIST 800-53 AC-3, IA-2

CONTENT TRANSFER		CONTENT TRANSFER TRACKING	
Description	Electronic transfer tools have logging capabilities enabled to monitor all transfer activities performed with digital content. Also, controls to ensure that logs are retained for an appropriate length of time are in place.		
Topics	Best Practices	Additional Considerations	Reference
Logging and Monitoring	<ul style="list-style-type: none"> • Enable electronic logging on content transfers to track and monitor digital assets as they are sent/received • Restrict administrative access rights (e.g., delete, copy, edit) to transfer logs to appropriate personnel (e.g., not personnel performing content transfers) 	<ul style="list-style-type: none"> • None 	ISO 27001: A.10.10.2, A.10.10.3 ISO 27002: 10.10 NIST 800-53 AU-3,6,9
Log Retention	<ul style="list-style-type: none"> • Retain audit logs for at least 90 days 	<ul style="list-style-type: none"> • None 	ISO 27001: A.10.10.1 ISO 27002: 10.1 NIST 800-53 AU-11

APPENDIX A – GLOSSARY

This glossary of basic terms and acronyms are most frequently used and referred to within this publication. These definitions have been taken from relevant ISO standards (27001/27002), security standards (i.e., NIST), and industry best practices.

Term or Acronym	Description
Access Control List (ACL)	Mechanism that implements access control for a system resource by listing the identities of the system entities that are permitted to access the resource
Access Rights	Permission to use/modify an object or system
Closed Circuit Television (CCTV)	Video cameras used to transmit a signal to a specific place on a limited set of monitors
CCTV Console	Central CCTV monitoring interface system
Digital Asset	Any form of content and/or media that have been formatted into a binary source which includes the right to use it
Dynamic Host Configuration Protocol (DHCP)	Protocol used to automatically assign IP addresses to all nodes on the network
Demilitarized Zone (DMZ)	Network created by connecting two firewalls, systems that are externally accessible but need some protection are usually located on DMZ networks
Encryption	Encryption is the conversion of data into a form, called a ciphertext, which cannot be easily understood by unauthorized people
Fingerprinting	Technique in which software identifies, extracts and then compresses characteristic components of a media, enabling that media to be uniquely identified by its resultant compressed form
Firewall	Gateway that limits access between networks in accordance with local security policy
Firewall Ruleset	Table of instructions that the firewall uses for determining how packets should be routed between source and destination
File Transfer Protocol (FTP)	TCP/IP protocol specifying the transfer of files across the network without encryption
Identification Badge	Card used to identify individuals authorized to access a facility (e.g., employees, vendors, visitors)
I/O Device	Devices used to communicate with and/or between computers (e.g., USB and FireWire drives)
IP Address	An Internet Protocol (IP) address is a numerical identification (logical address) that is assigned to devices participating in a computer network
Keycard	Plastic card which stores a digital signature that is used with electronic access control locks
Local Area Network (LAN)	Computer network covering a small physical area (e.g., an office)
MAC Address Filtering	Security access control methodology used to determine access to a computer network

Term or Acronym	Description
Master Key	Keys that offer access to all doors (interior and exterior) at any given facility. Also, keys with access to all high security areas are considered to be Master Keys
Media	Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, LSI memory chips, printouts onto which information is recorded, stored, or printed within an information system
Network Protocol	Convention or standard that controls or enables the connection, communication, and data transfer between computing endpoints
Office Network	Computer network covering a particular work space
Production Network	The 'live' instance of a computer network that is used by a majority of the employees
Release Window	The time frame a film is released to the public through a specific media, (i.e., theatrical, home video, premium TV, etc.)
Router	Device whose software and hardware is tailored to the tasks of steering and forwarding information
Small Computer System Interface (SCSI)	Standards for physically connecting and transferring data between computers and peripheral devices
Static IP	Configuration wherein a computer uses the same IP address each time it powers up
Switch	Computer networking device that connects the network with segments through network cables
Telnet	Network Protocol used on the Internet or local area network
Tracking Mechanisms	Tools, processes, and/or methods used to track assets throughout the production process, including asset registration, tracking of asset movements (e.g., move an asset from vault to edit bays), shipping, and asset destruction
Transfer Tools	Tools used for the electronic transmission of digital assets through a network. Common tools that use acceptable encryption and authentication mechanisms include: Aspera, WAM!NET, DigiDelivery
Transfer Protocol	The procedure involved in transmitting files over a computer network or the Internet
Unique Username	Distinguishable login identification
Universal Serial Bus (USB)	Serial bus standard to connect devices to a host computer
User Access Management	The process of creating, changing access rights, and removing user accounts from a system or application
Virtual Local Area Network (VLAN)	Computer network having the attributes of a LAN but not limited to physical location
Virtual Private Network (VPN)	Computer network that allows users to access another larger network
Wide Area Network (WAN)	Computer network covering a broad area (e.g., a company)
Watermarking	The process of (possibly) irreversibly embedding information into a digital asset
Work in Progress (WIP)	Any good that is not considered to be a final product

APPENDIX B – FREQUENTLY ASKED QUESTIONS

1. Is my facility required to implement all of the best practices presented?

Compliance with best practices is strictly voluntary. They are suggested guidelines to consider when planning, implementing, and modifying security procedures. Security constraints must take into account workflow and cost considerations.

2. If my facility offers multiple services (e.g., creative advertising and post-production), what set of best practices should I apply?

Facilities should always apply the more restrictive set of best practices.

3. If implementing best practices listed in this guideline, will my facility be ranked with the highest maturity level if surveyed?

Not necessarily. Best practices are intended for facilities to improve security at their facility; they do not necessarily set the standard at the highest maturity level in the MPAA Content Security Maturity Model. If there is an MPAA site survey of a facility, the “best practice” for a given facility type will not necessarily be classified at the highest maturity level in the model.

4. What if my current system does not allow for the implementation of best practices?

Please contact the respective vendor in order to identify possible solutions to enable systems to follow best practices. Solutions can include patching, updating version, or even changing to a more secure system. Alternative controls can also be implemented if technical limitations prevent the implementation of best practices; however, these are normally not considered to fully cover the associated risks.

Exceptions to the implementation of security policies due to system limitations should be formally documented and approved.

5. When applying best practices in this guideline, will my facility still need to comply with security requirements set individually by an MPAA Member Company?

The implementation of best practices is a guideline and does not supersede specific contractual provisions with individual MPAA Member Companies. Decisions regarding the use of vendor(s) by any particular Member Company are made by each Member Company solely on a unilateral basis. We encourage you to use the best practices as a guideline for future discussions around security with your clients.

6. Is there a standard physical asset tracking tool that covers basic requirements from best practices?

Best practices are not based on and do not promote a specific technology or application; however, the following are common tools used across several facilities for the tracking of physical assets: Xytech Systems, ScheduALL, SmartTurn, and Artesia.

APPENDIX C – SUGGESTED POLICIES AND PROCEDURES

The following list presents some common areas for which security policies and procedures should be considered to aid companies to safeguard client assets and digital content.

1. Physical Security Policies and Procedures

- Entry/exit points security
- Visitor access protocol
- Identification and authorization
- Emergency protocol
- Facility access controls
- Facility monitoring

2. Inventory and Asset Management

- Inventory tracking
- Blank media/raw stock control
- Asset disposal
- Shipping and receiving
- Inventory storage/vaulting

3. Information Technology Security

- Network and perimeter security
- Remote access
- Internet usage policy
- Wireless usage policy
- System security policies
- Administrative access rights policy
- Authentication and authorization
- Password policy
- System hardening – minimum security baselines
- Malicious code protection/anti-virus
- Security monitoring and logging
- Secure transmission of digital content
- Secure storage of digital content

4. Human Resources Policies and Procedures

- Including security in job responsibilities
- Personnel screening
- Confidentiality, property rights, and intellectual property protection agreements
- Terms and conditions of employment
- Segregation of duties
- Termination of employment
- Disciplinary measures

- Security awareness and training program
 - Employee and temp/freelancer background/reference checks and screening
 - Employee and temp/freelancer non-disclosure agreements (NDAs)
5. **Third Parties**
- Third party contracts
 - Non-disclosure agreements
6. **Incident Response:**
- Incident identification and analysis
 - Incident escalation and reporting
 - Incident response processes and procedures
 - Post mortem review procedures and lessons learned

APPENDIX D – BIBLIOGRAPHY

[1] International Organization for Standardization (ISO), Standard 27001. *Information technology - Security techniques - Information security management systems – Requirements*. October 2005.

<http://www.27000.org/iso-27001.htm>

[2] International Organization for Standardization (ISO), Standard 27002. *Information technology - Security techniques - Code of practice for information security management*. July 2007.

<http://www.27000.org/iso-27002.htm>

[3] International Organization for Standardization (ISO), Standard 27005. *Information technology - Security technique- Information security risk management*. June 2008.

<http://www.27000.org/iso-27005.htm>

[4] National Institute of Standards and Technology Special Publication 800-53. *Recommended Security Controls for Federal Information Systems*, February 2005.

<http://csrc.nist.gov/publications/drafts/800-53/800-53-rev3-IPD.pdf>

[5] National Institute of Standards and Technology Special Publication IR 7298. *Glossary of Key Information Security Terms*, April 2006.

http://csrc.nist.gov/publications/nistir/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf

[6] SysAdmin, Audit, Networking, and Security (SANS Institute). *Glossary of Terms Used in Security and Intrusion Detection*

<http://www.sans.org/resources/glossary.php#m>

APPENDIX E – MPAA 24-HOUR TIP LINE

The following list presents the 24-hour tip line contact information for the respective region and country.

Country	24-Hour Tip Line
<i>North America and Latin America Region</i>	
Canada, French and English	(800) 363-9166
United States	(800) 371-9884
<i>Europe, Middle East, Africa (EMEA) Region</i>	
Belgium, English	+32 2 463 15 10
Belgium, French	+35 22 482 85 87
Italy	800 864 120
Netherlands	909 747 2837
Ukraine	+38 0 445 013829
United Kingdom	800 555 111
<i>Asia Pacific (APAC) Region</i>	
Australia	+61 2 9997 8011
Hong Kong	+65 6253-1033
Malaysia	+65 6253-1033
New Zealand	+65 6253-1033
Philippines	+65 6253-1033
Singapore	+65 6253-1033
Taiwan	+65 6253-1033