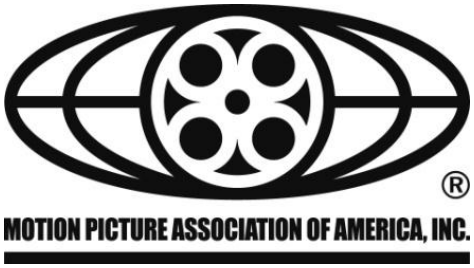


MPAA Site Security Program

CONTENT SECURITY BEST PRACTICES COMMON GUIDELINES

www.fightfilmtheft.org/en/bestpractices/_piracyBestPractice.asp

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

TABLE OF CONTENTS

I. Best Practices Overview

Introduction

For more than three decades, the Motion Picture Association of America, Inc. (MPAA) has managed site security surveys on behalf of its Member Companies (Members): Walt Disney Studios Motion Pictures; Paramount Pictures Corporation; Sony Pictures Entertainment Inc.; Twentieth Century Fox Film Corporation; Universal City Studios LLC; and Warner Bros. Entertainment Inc.

Starting in 2007, these reviews were performed using a standardized survey model, process and report template. Since then, over 300 facilities have been surveyed in 32 countries.

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 stake in protecting intellectual property rights and recognizing that these safeguards are a cornerstone of a healthy global information economy.

The MPAA Site Security Program's purpose is to strengthen the process by which its Member content is protected during production, post-production, marketing and distribution. This is accomplished by:

- Publishing a set of best practices by facility service outlining standard controls that help to secure Member content;
- Assessing and evaluating content security at third-party partners based on published best practices;
- Reinforcing the importance of securing Member content; and
- Providing a standard survey vehicle for further individual discussions regarding content security between Member and their business partners.

Purpose and Applicability

The purpose of this document is to provide current and future third party vendors engaged by Members with an understanding of general content security expectations and current industry best practices. Decisions regarding the use of vendors by any particular Member are made by each Member solely on a unilateral basis.

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

Best practices outlined in this document are subject to local, state, regional, federal and country laws or regulations.

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.

Exception Process

Where it may not be feasible to meet a best practice, facilities should document why they cannot meet the best practice and implement compensating measures used in place of the best practice. Exceptions should also be communicated directly to the Member.

Questions or Comments

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

II. FACILITY OVERVIEW

The following table describes the typical services offered, content handled and release window involved with each facility type.

No.	Facility Type	Typical Facility Services	Type of Content	Release Window
1	**Audio, Dubbing and Sub-Titling**	•Original and Foreign Language Dubbing •Subtitling •SFX •Scoring •ADR/Foley	•Low-Resolution •Watermarked/Spoiled •Full/Partial Feature Content •Audio Masters	• Pre-Theatrical • Pre-Home Video
2	**Courier, Delivery and Freight**	•Courier Services •Delivery Services •Shipping Companies	•Varied	• Pre-Theatrical • Pre-Home Video • Catalog
3	**Creative Advertising**	•Non-Finishing •Trailer •TV Spots •Teasers •Graphics •Web Ads	•Watermarked, Spoiled Full/Partial Feature Content •Stills •Clips	• Pre-Theatrical • Pre-Home Video • Catalog
4	**Digital Cinema**	•Digital Cinema Mastering •Replication •Key Management	•High-Resolution – Full or Partial Content •Digital Cinema Distribution Masters •Digital Cinema Packages	• Pre-Theatrical
5	**Digital Services**	•Digital Intermediate •Scanning •Film Recording •Film Restoration	•Clean and High Resolution – Full or Partial Content (Film Tape)	• Pre-Theatrical • Catalog
6	**Distribution**	•Distribution •Fulfillment •Backroom/Film Depot •DVD/Tape Recycling	•High Resolution •Clean Image	• Pre-Theatrical • Pre-Home Video • Catalog
7	**DVD Creation**	•Compression •Authoring •Encoding •Regionalization •Special Features •Check Disc QC	•Clean – Full Feature	• Pre-Home Video
8	**Film Lab**	•Negative Processing •Cutting •Release Prints	•Clean – Full Feature	• Pre-Theatrical
9	**In Flight Entertainment (IFE) and Hospitality Services**	•IFE Lab •IFE Integration •Hotel •Airline •Cruise Ship/Ferry •Libraries •Hospitals •Prisons	•High-Resolution – Full or Partial Content •Spoiled – Full or Partial Content	• Pre-Theatrical • Pre-Home Video • Catalog
10	**Post-Production Services**	•Telecine •Duplication •Editing •Finishing •QC	•High-Resolution – Full or Partial Content	• Pre-Theatrical • Pre-Home Video • Catalog
11	**Replication**	•Pre-Mastering •Mastering •Replication •Check Disc Creation	•High Resolution •Clean Image	• Pre-Home Video
12	**Visual Effects (VFX)**	•Digital Post-Production •Computer Generated Imagery •Animation	•High-Resolution – Partial •Frames, Shots, Sequences and Stills •Scripts •Storyboards	• Pre-Theatrical • Post-Theatrical (2D to 3D)

III. Risk Management

Risk Assessment

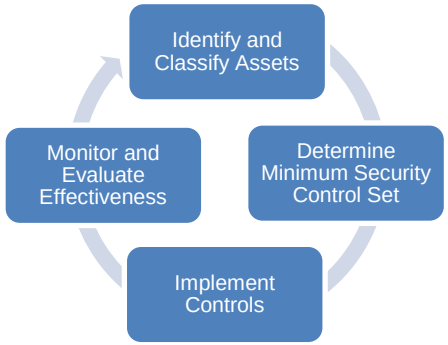
Risks should be identified through a risk assessment, and appropriate controls should be implemented to decrease risk to an acceptable level and ensure that business objectives are met.

The International Organization for Standardization (ISO) 27000 defines risk as the "combination of the probability of an event and its consequence." For example, what is the probability that content can be stolen from a facility's network and released publicly and what is the business consequence to an organization and the client if this occurs (e.g., contractual breech and/or loss of revenue for that release window).

The importance of a robust management system is also highlighted in the ISO 27001 standard that shows how to establish an Information Security Management System (ISMS).

Asset Classification

One way to classify assets at your facility is to follow a four-step process, which is summarized below:



In consultation with the Member (its client), an organization is responsible for determining which client assets require a higher level of security. The following table provides an example of how to classify content:

Classification	Description	Examples
High-Security Content	Any content that the organization believes would result in financial loss, negative brand reputation, or serious penalties should the asset be stolen or leaked	• Theft of a blockbuster feature before its first worldwide theatrical release • Theft of home video content before its first worldwide street date • Theft of masters or screeners

Additional information about risks generally associated with each facility type is also included in each supplemental best practice.

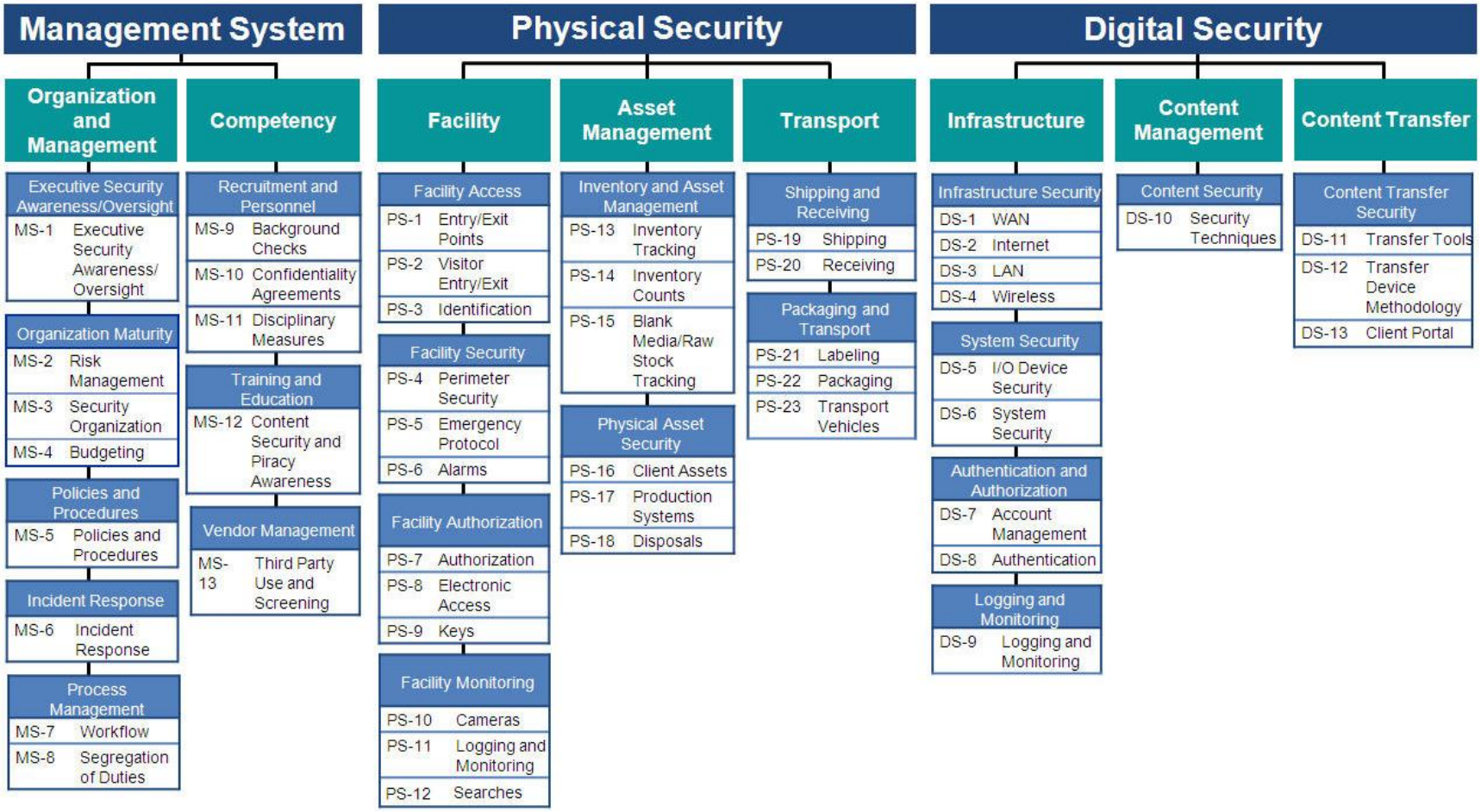
Security Controls

The IT Governance Institute defines controls as "the policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected." Security controls are typically selected based on the classification of the asset, its value to the organization, and the risk of the asset being leaked or stolen.

In order to mitigate identified risks, organizations are encouraged to implement controls commensurate to each specific risk. Such measures should also be evaluated periodically for their design and effectiveness based on the current threat environment.

IV. Document Organization

Best practices are organized according to the MPAA Content Security Model, which provides a framework for assessing a facility's ability to protect a client's content. It is comprised of 49 security topics across three areas: management system, physical security and digital security. The components of the MPAA Content Security Model are drawn from relevant ISO standards (27001/27002), security standards (i.e., NIST) and industry best practices.



V. BEST PRACTICES FORMAT

Best practices are presented for each security topic listed in the MPAA Content Security Model using the following format:

MANAGEMENT SYSTEM		PHYSICAL SECURITY			DIGITAL SECURITY		
ORGANIZATION AND MANAGEMENT	COMPETENCY	FACILITY	ASSET MANAGEMENT	TRANSPORT	INFRASTRUCTURE	CONTENT MANAGEMENT	CONTENT TRANSFER

The chart at the top of every page highlights the security area being addressed within the overall MPAA Content Security Model.

No.	Security Topic	Best Practice	Implementation Guidance
PS-9.0	Keys	Limit the distribution of **master keys** to authorized personnel only (e.g., owner, facilities management)	• Maintain a list of **company personnel** who are allowed to check out **master keys** • Update the list regularly to remove any **company personnel** who no longer require access to **master keys**
PS-9.1		Implement a check-in/check-out process to track and monitor the distribution of **master keys**	• Maintain records to track the following information: – **Company personnel** in possession of each **master key** – Time of check-out/check-in – Reason for check-out

No.

Each best practice is assigned a reference number in the form of XX-Y.Z. XX for the general area, Y for the Security Topic, and Z for the specific control.

Security Topic

Each capability area is comprised of one of more "Security Topics." Each Security Topic is addressed with one or more best practices.

Best Practice

Best practices are outlined for each Security Topic.

Implementation Guidance

Additional considerations, potential implementation steps and examples are provided to help organizations implement the best practices.

Glossary

All terms that are included in the glossary are highlighted in **bold** and defined in Appendix A.

VI. BEST PRACTICE COMMON 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-1.0	Executive Security Awareness/ Oversight	Ensure executive management/owner(s) oversight of the Information Security function by requiring periodic updates of the information security program and **risk assessment** results	
MS-1.1		Train and engage executive management/owner(s) on the business' responsibilities to protect content	
MS-2.0	Risk Management	Develop a formal security **risk assessment** process focused on content **workflows** and sensitive assets in order to identify and prioritize risks of content theft and leakage that are relevant to the facility	• Define a clear scope for the security **risk assessment** • Incorporate a systematic approach that uses likelihood of risk occurrence, impact to business objectives/content protection and asset classification for assigning priority
MS-2.1		Identify high-security content based on client instruction	
MS-2.2		Perform a security **risk assessment** annually, update the **risk assessment** when key **workflows** change, and document and act upon identified risks	• Conduct meetings with management and key stakeholders to identify and document content theft and leakage risks • Identify key risks that reflect where the facility believes content losses may occur • Consider performing a threat and vulnerability assessment to identify existing risks • Update **risk assessment** to reflect additional risks when **workflows** change • Implement and document controls to mitigate or reduce identified risks • Monitor and assess the effectiveness of remediation efforts and implemented controls at least annually

No.	Security Topic	Best Practice	Implementation Guidance
MS-3.0	Security Organization	Identify security key point(s) of contact and formally define roles and responsibilities for content and asset protection	• Prepare organization charts and job descriptions to facilitate the designation of roles and responsibilities as it pertains to content security • Provide online or live training to prepare security personnel on policies and procedures that are relevant to their job function
MS-4.0	Budgeting	Document and budget for security initiatives, upgrades, and maintenance	• Develop a formal budget for security-related initiatives • Maintain a reserve budget for emergencies • Include the following when developing the security budget: – Physical security systems (e.g., **CCTV**, alarm systems) – Information technology security systems (e.g., proxy servers, **firewalls**) – Maintenance of existing security systems – New security initiatives
MS-5.0	Policies and Procedures	Establish policies and procedures regarding asset and content security; policies should address the following topics, at a minimum: • Human resources policies • Acceptable use (e.g., social networking, Internet, phone, etc.) • Asset classification • Asset handling policies • Digital recording devices (e.g., smart phones, digital cameras, camcorders) • Exception policy • Password controls (e.g., password minimum length, screensavers) • Prohibition of client asset removal from the facility • System change management • Whistleblower policy	• Require management to sign off on all policies and procedures before they are published and released • Please see Appendix E for the complete list of policies and procedures to consider

No.	Security Topic	Best Practice	Implementation Guidance
MS-5.1		Review and update security policies and procedures at least annually	• Incorporate the following factors into the annual managerial review of security policies and procedures: – Recent security trends – Feedback from **company personnel** – New threats and vulnerabilities – Recommendations from regulatory agencies (i.e., FTC, etc.) – Previous security incidents
MS-5.2		Require a sign-off from all **company personnel** (e.g., employees, temporary workers, interns) and **third party workers** (e.g., contractors, freelancers, temp agencies) for all policies, procedures, and/or client requirements and any updates	• Distribute copies of the company handbook containing all general policies and procedures upon hire of new **company personnel** and **third party workers** • Notify **company personnel** and **third party workers** of updates to security policies and procedures through email • Provide digital copies of current policies and procedures via shared drive or intranet
MS-6.0	Incident Response	Establish a formal **incident response** plan that describes actions to be taken when a security incident is detected and reported	• Consider including the following sections in the **incident response** plan: – Detection of incident – Notification of security team – Escalation to management – Analysis of impact and priority – Containment of impact – Eradication and recovery – Key contact information • Identify, prioritize, and document a list of types of incidents that are likely to occur and include procedures for handling each type of incident in the security **incident response** plan • Reference NIST SP800-61 on Computer Security Incident Handling

No.	Security Topic	Best Practice	Implementation Guidance
MS-6.1		Identify the security **incident response** team who will be responsible for detecting, analyzing, and remediating security incidents	• Include representatives from different business functions in order to address security incidents of all types; consider the following: – Management – Physical security – Information security – Network team – Human resources – Legal • Provide training so that members of the **incident response** team understand their roles and responsibilities in handling incidents
MS-6.2		Establish a security incident reporting process for individuals to report detected incidents to the security **incident response** team	• Consider implementing an anonymous hotline or website that can be used to report inappropriate and/or suspicious activity • Consider leveraging the MPAA tips hotline for anonymous tips on suspicious activity – please refer to the 24-hour tip hotline contact information in Appendix G
MS-6.3		Communicate incidents to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client assets), and conduct a post-mortem meeting with management and client	• Implement a security breach notification process, including the use of breach notification forms • Involve the Legal team to determine the correct actions to take for reporting content loss to affected clients • Discuss lessons learned from the incident and identify improvements to the **incident response** plan and process • Perform root cause analysis to identify security vulnerabilities that allowed the incident to occur • Identify and implement remediating controls to prevent similar incidents from reoccurring • Communicate the results of the post-mortem, including the corrective action plan, to affected clients

No.	Security Topic	Best Practice	Implementation Guidance
MS-7.0	Workflow	Document a **workflow** that includes the tracking of content and authorization checkpoints throughout each process; include the following processes for both physical and digital content: • Delivery • Ingest • Movement • Storage • Return to originator • Removal from the site • Destruction	• Use swim lane diagrams (e.g., Visio diagrams) to document the **workflow** • Include asset processing and handling information where applicable • Include controls around authorization checkpoints • Consider identifying applications controls (e.g., completeness, accuracy, validity, restricted access) in the **workflow**
MS-7.1		Identify, implement, and assess the effectiveness of key controls to prevent, detect, and correct risks related to the content **workflow**	• Follow the content **workflow** and implemented controls for each process in order to determine areas of vulnerability • Incorporate identified risks into the **risk management** process to assess, prioritize, and address content **workflow** risks • Identify key control points in the **workflow** process • Maintain a chain of custody form that is transmitted along with each asset as it moves through the **workflow** • Establish an independent team to perform periodic auditing of the **workflow** • Review the **workflow** process annually to identify security improvements with the **workflow** process, if any

No.	Security Topic	Best Practice	Implementation Guidance
MS-8.0	Segregation of Duties	Segregate duties within the content **workflow**	• Document roles and responsibilities to eliminate an overlap of role-based job functions such as: – **Vault** and server/machine room personnel – Shipping and receiving personnel – Asset movement within facility (e.g., runners) from **vault** and content/production area – **Digital asset** folder access (e.g., data wrangler sets up access for producer) – Content transfer personnel from production personnel • Segregate duties using manual controls (e.g., approval from producer before working on content) or automated controls in the work ordering system (e.g., automated approval for each stage of the **workflow**)
MS-8.1		Implement and document compensating controls where segregation is not practical	• Implement compensating controls when segregation is unattainable, such as: – Monitor the activity of **company personnel** and/or **third party workers** – Retain and review audit logs – Implement physical segregation – Enforce management supervision

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-9.0	Background Checks	Perform background screening checks on all **company personnel** and **third party workers**	• Carry out background checks in accordance with relevant laws, regulations, union bylaws, and cultural considerations • Screen potential **company personnel** and **third party workers** using background screening checks that are proportional to the business requirements, the sensitivity of content that will be accessed, and possible risks of content theft or leakage • Perform identity, academic, and professional qualification checks where necessary • Where background checks are not allowed by law, document as an exception and use reference checks
MS-10.0	Confidentiality Agreements	Require all **company personnel** and **third party workers** to sign a confidentiality agreement (e.g., non-disclosure) upon hire and annually thereafter, that includes requirements for handling and protecting content	• Include non-disclosure guidance pertaining to confidentiality after termination of their employment, contract, or agreement • Explain the importance of confidentiality/NDA in non-legal terms, as necessary
MS-10.1		Require all **company personnel** and **third party workers** to return all content and client information in their possession upon termination of their employment or contract	• Ensure all relevant information on equipment used by **company personnel** and **third party workers** to handle business-related sensitive content is transferred to the organization and securely removed from the equipment

No.	Security Topic	Best Practice	Implementation Guidance
MS-11.0	Disciplinary Measures	Define and communicate disciplinary measures for violations of facility policies to all **company personnel** and **third party workers**	• Identify appropriate disciplinary measures that are commensurate with the severity and business impact of any security-related breaches caused by the individual • Involve senior management in determining the actions to be applied • Communicate potential sanctions to all **company personnel** and **third party workers** • Document the measures in the company handbook, security policies and other areas • Communicate disciplinary measures in new hire orientation training
MS-12.0	Content Security and Piracy Awareness	Develop and regularly update a security awareness program and train **company personnel** and **third party workers** upon hire and annually thereafter, addressing the following areas at a minimum: • IT security policies and procedures • Content/asset security and handling • Security incident reporting and escalation • Disciplinary measures	• Distribute security awareness materials such as posters, e-mails, and periodic newsletters to encourage security awareness • Communicate security awareness messages during management/staff meetings • Developed tailored messages and training based on job responsibilities (e.g., IT personnel, production) • Require suitable levels of security training for different **company personnel** depending on the individual's responsibilities and interaction with sensitive content • Provide online or in-person training upon hire to educate **company personnel** and **third party workers** about common incidents, corresponding risks, and their responsibilities for reporting detected incidents • Implement procedures to track which **company personnel** have completed their annual security training (e.g., database repository, attendee logs, certificates of completion) • Consider recording training sessions and making recordings available for reference
MS-13.0	Third Party Use and Screening	Require all **third party workers** who handle content to sign confidentiality agreements (e.g., non-disclosure) upon engagement	• Include non-disclosure guidance in policies pertaining to confidentiality during and after their employment, contract, or agreement

No.	Security Topic	Best Practice	Implementation Guidance
MS-13.1		Include security requirements in third party contracts	• Require **third party workers** to comply with the security requirements specified in third party contracts and client requirements • Include a right to audit clause for activities that involve sensitive content • Implement a process to monitor for compliance with security requirements
MS-13.2		Implement a process to reclaim assets and remind **third party workers** of confidentiality agreements and contractual security requirements when terminating relationships	• Ensure all relevant information third party equipment that is used to handle business-related sensitive content is transferred to the organization and securely erased from the equipment
MS-13.3		Require **third party workers** to be bonded and insured where appropriate (e.g., courier service)	• Require **third party workers** to show proof of insurance and keep a record of their insurance provider and policy number • Require third party insurance to meet a certain level of coverage • Require annual update of information when contracts are renewed
MS-13.4		Restrict third party access to content/production areas unless required for their job function	• Ensure that **third party workers** are not given electronic access to areas housing content • Escort **third party workers** (e.g., cleaning crews) when access to restricted areas (e.g., **vault**) is required
MS-13.5		Require third party companies to notify clients if they are on-boarding additional third party companies to handle content	• Create a form to be used for notifying clients of additional third party usage and require client sign-off for approval • Require the additional third party companies to go through standard **due diligence** activities for **third party workers**

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-1.0	Entry/Exit Points	Lock all entry/exit points at all times if the facility does not have a segregated access-controlled area beyond reception	• Permit entry/exit points to be unlocked during business hours if the reception area is segregated from the rest of the facility with access-controlled doors
PS-1.1		Control access to production areas by segregating the content/production area from other facility areas (e.g., administrative offices)	• Allow access to content/production areas on a need-to-know basis
PS-1.2		Require rooms used for screening purposes to be access-controlled (e.g., projection booths)	• Limit access into rooms where **media** players are present (e.g., Blu-ray, DVD)
PS-2.0	Visitor Entry/Exit	Maintain a detailed visitors' log which includes the following: • Name • Company • Time in/time out • Person/people visited • Signature of visitor • Badge number assigned	• Verify the identity of all visitor by requiring them to present valid photo identification (e.g., driver's license, studio badge, government-issued ID) • Consider concealing the names of previous visitors
PS-2.1		Assign an **identification badge** or sticker, which must be visible at all times, to each visitor and collect badges upon exit	• Make visitor badges easily distinguishable from **company personnel** badges (e.g., color coded plastic badges) • Consider a daily rotation for paper badges or sticker color • Consider using badges that change color upon expiration • Log badge assignments upon entry/exit • Visitor badges should be sequentially numbered and tracked • Account for badges daily
PS-2.2		Do not provide visitors with electronic access to content/production areas	

No.	Security Topic	Best Practice	Implementation Guidance
PS-2.3		Require visitors to be escorted by authorized employees while on-site, or in content/production areas at a minimum	• Do not allow visitors to enter the facility beyond the front desk until the appropriate **company personnel** arrives to escort the visitor • Do not leave visitors alone in content/production areas
PS-3.0	Identification	Provide **company personnel** and long-term **third party workers** (e.g., janitorial) with photo identification that is validated and required to be visible at all times	• Issue photo ID to all **company personnel** and long-term **third party workers** after a background check has been completed • Establish and implement a process for immediately retrieving photo ID upon termination • Consider omitting location and other specific information on the photo ID • Consider using the photo ID as the access key card where possible • Require employees to immediately report lost or stolen photo ID • Provide a 24/7 telephone number or website to report lost or stolen photo ID
PS-4.0	Perimeter Security	Implement perimeter security controls that address risks that the facility may be exposed to as identified by the organization's **risk assessment**	• Implement security controls based upon the location and layout of the facility, such as: – 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 – Placing security guards at entry/exit points – 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 – Being cognizant of the overuse of company signage that could create targeting – Using alarms around the perimeter, as necessary

No.	Security Topic	Best Practice	Implementation Guidance
PS-5.0	Emergency Protocol	Install a power backup system (e.g., Uninterruptible Power Supply or "UPS") to support security installations (e.g., **CCTV** system, alarm system, electronic access system) and critical production systems for at least 15 minutes to allow enough time for the facility to be secured upon an emergency, incident, or power outage	• Install individual power supplies for each of the security systems in place (e.g., alarm, **CCTV**, electronic access system) if a UPS is not available • Configure automatic shutdown of production systems upon extended power outage • Incorporate SMS messaging devices
PS-5.1		Test and conduct maintenance for the power backup system at least annually	• Establish the length of time the UPS and/or Power Generator can supply power for an average system load to help ensure sufficient time to save and shutdown • Keep records of maintenance and testing
PS-5.2		Configure electronic access systems, when implemented at the facility, as fail-secure in case of a power outage	• Ensure that doors allow individuals to exit the facility during power outages but still require positive authentication to enter
PS-6.0	Alarms	Install a centralized, audible alarm system that covers all entry/exit points (including emergency exits), loading docks, fire escapes, and restricted areas (e.g., **vault**, server/machine room)	• Place alarms at every entrance to alert security personnel upon unauthorized entry to the facility • Enable the alarm at all times
PS-6.1		Configure alarms to provide escalation notifications directly to the personnel in charge of security and/or be monitored by a central security group or third party	• Establish and implement escalation procedures to be followed if a timely response is not received from security personnel upon notification • Consider implementing automatic law enforcement notification upon breach • Implement procedures for notification on weekends and after business hours
PS-6.2		Assign unique arm and disarm codes to each person that requires access to the alarm system and restrict access to all other personnel	• Use unique alarm codes to track which security personnel was responsible for arming/disarming the alarm • Update assigned alarm codes at an interval approved by management in order to reduce risk involved with sharing and losing codes

No.	Security Topic	Best Practice	Implementation Guidance
PS-6.3		Review the list of users who can arm and disarm alarm systems annually	• Remove users who have left the company or have changed job roles • Deactivate the alarm codes that were assigned to removed users
PS-6.4		Test the alarm system every 6 months	• Simulate a breach in physical security and ensure the following: – Alarm system detects the breach – Security personnel are alerted – Security personnel respond in a timely manner according to procedures
PS-6.5		Install and effectively position motion detectors in restricted areas (e.g., **vault**, server/machine room) and configure them to alert the appropriate security personnel and/or third-party	• Ensure the alarm system covers storage areas and **vaults** (e.g., through motion sensors) after normal business hours, as an added layer of security
PS-6.6		Install door prop alarms for content/production areas to notify when sensitive entry/exit points are open for longer than a pre-determined period of time (e.g., 60 seconds)	• Configure access-controlled doors to trigger alarms and alert security personnel when doors have been propped open for an extended period of time
PS-7.0	Authorization	Document and implement a process to manage facility access and keep records of any changes to **access rights**	• Designate an individual to authorize facility access • Notify appropriate personnel (e.g., facilities management) of changes in employee status • Create a physical or electronic form that must be filled out by a supervisor to request facility access for **company personnel** and/or **third party workers** • Assign responsibility for investigating and approving access requests
PS-7.1		Review access to restricted areas (e.g., **vault**, server/machine room) quarterly and when the roles or employment status of **company personnel** and/or **third party workers** are changed	• Validate the status of **company personnel** and **third party workers** Remove **access rights** from any terminated users • Verify that access remains appropriate for the users' associated job function

No.	Security Topic	Best Practice	Implementation Guidance
PS-8.0	Electronic Access	Implement electronic access throughout the facility to cover all entry/exit points and all areas where content is stored, transmitted, or processed	• Assign electronic access to specific facility areas based on job function and responsibilities • Update electronic access accordingly when roles change or upon termination of **company personnel** and **third party workers** • Keep a log that maps **keycard** number to **company personnel** • Review the times when electronic access is not required for common areas (e.g., public elevators)
PS-8.1		Restrict electronic access system administration to appropriate personnel	• Restrict electronic system administration to designated personnel and do not allow individuals who have access to production content to perform administrative electronic access tasks • Assign an independent team to administer and manage electronic access
PS-8.2		Store blank card stock in a locked cabinet and ensure **keycards** remain disabled prior to being assigned to personnel	• Limit access to the locked cabinet to the **keycard** system administration team • Require sign-out for inventory removal
PS-8.3		Disable lost **keycards** in the system before issuing a new **keycard**	• Educate **company personnel** and **third party workers** to report lost **keycards** immediately to prevent unauthorized access into the facility • Require identification before issuing replacement **keycards**
PS-8.4		Remove physical locks for restricted areas (e.g., **vault**, server/machine room) where an electronic access system is implemented	
PS-8.5		Issue third party access cards with a set expiration date (e.g. 90 days) based on an approved timeframe	• Ensure that third party access cards are easily distinguishable from **company personnel** access cards (e.g., color coded) • Ensure that expiration date is easily identifiable on the access cards • Assign third party **keycard** access on a need-to-know basis

No.	Security Topic	Best Practice	Implementation Guidance
PS-9.0	Keys	Limit the distribution of **master keys** to authorized personnel only (e.g., owner, facilities management)	• Maintain a list of **company personnel** who are allowed to check out **master keys** • Update the list regularly to remove any **company personnel** who no longer require access to **master keys**
PS-9.1		Implement a check-in/check-out process to track and monitor the distribution of **master keys**	• Maintain records to track the following information: – **Company personnel** in possession of each master key – Time of check-out/check-in – Reason for check-out • Require **master keys** to be returned within a set time period and investigate the location of keys that have not been returned on time
PS-9.2		Use keys that can only be copied by a specific locksmith for exterior entry/exit points	• Ensure the keys are engraved with "Do Not Duplicate" • Use high-security keys (cylinders) that offer a greater degree of resistance to any two or more of the following: – Picking – Impressioning – Key duplication – Drilling – Other forms of forcible entry
PS-9.3		Inventory **master keys** and keys to restricted areas, including facility entry/exit points, quarterly	• Identify, investigate, and address any missing keys • Review logs to determine who last checked out a key that cannot be accounted for • Change the locks when missing **master keys** or keys to restricted areas cannot be accounted for
PS-10.0	Cameras	Install a **CCTV** system that records all facility entry/exit points and restricted areas	
PS-10.1		Implement controls to ensure that camera footage is clear and visible in all lighting conditions	• Accommodate for cameras in dark areas (e.g., low-light or infrared cameras, motion-detecting lights) • Adjust image quality adequately to positively identify individuals

No.	Security Topic	Best Practice	Implementation Guidance
PS-10.2		Restrict physical and logical access to the **CCTV console** and to **CCTV** equipment (e.g., DVRs) to personnel responsible for administering/monitoring the system	• Place **CCTV** equipment in a secure access-controlled location (e.g., computer room, locked closet, cage) • Perform periodic access reviews to ensure that only the appropriate individuals have access to surveillance equipment • Ensure that the web console for IP-based **CCTV** systems is restricted to authorized personnel and that strong account management controls are in place (e.g., password complexity, individual user login, logging and monitoring)
PS-10.3		Review camera positioning, image quality, frame rate, and adequate retention of surveillance footage weekly	• Review camera positioning to ensure an unobstructed view of all entry/exit points and other sensitive areas • Review image quality to ensure that lighting is adequate and that faces are distinguishable • Review frame rate to ensure that the footage adequately captures activity • Review surveillance footage to ensure that footage is being retained for at least 90 days • Position cameras to avoid capturing content on display
PS-10.4		Ensure that camera footage includes an accurate date and time-stamp	• Burn the time and date onto the physical **media** for camera footage recorded on tape or disk • Ensure that accurate time-stamps are maintained on the recording equipment for digital camera footage
PS-11.0	Logging and Monitoring	Log and review electronic access to restricted areas for suspicious events	• Identify and document a set of events that are considered suspicious • Consider the implementation of an automated reporting process that sends real-time alerts to the appropriate security personnel when suspicious electronic access activity is detected • Log and review the following events: – Repeated failed access attempts – Unusual time-of-day access – Successive door access across multiple zones

No.	Security Topic	Best Practice	Implementation Guidance
PS-11.1		Investigate suspicious electronic access activities that are detected	• Identify and communicate key contacts that should be notified upon detection of unusual electronic access activity • Establish and implement escalation procedures that should be followed if primary contacts do not respond to event notification in a timely manner
PS-11.2		Maintain an ongoing log of all confirmed electronic access incidents and include documentation of any follow-up activities that were taken	• Leverage the **incident response** reporting form to document confirmed **keycard** incidents • Review all recent **keycard** incidents periodically and perform root-cause analysis to identify vulnerabilities and appropriate fixes
PS-11.3		Retain **CCTV** surveillance footage and electronic access logs for at least 90 days, or the maximum time allowed by law, in a secure location	• Consider storing logs in an access-controlled telecom closet or computer room • Determine the typical amount of space required for one day of logging and ensure that the log size is large enough to hold records for at least 90 days, or the maximum retention period allowed by law
PS-12.0	Searches	Inform **company personnel** and **third party workers** upon hire that bags and packages are subject to random searches and include a provision addressing searches in the facility policies	• Communicate policies regarding search to all **company personnel** and **third party workers** • Conduct searches periodically of **company personnel** and **third party workers** to validate policy

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-13.0	Inventory Tracking	Implement a content **asset management** system to provide detailed tracking of physical assets (i.e., client and newly created)	• Require a release form or work order to confirm that content can be checked out by a specific individual • Require individuals to present identification for authentication • Require a tag (e.g., barcode, unique ID) for all assets • Log all assets that are checked-in/checked-out • Log the expected duration of each check out • Track and follow up with individuals that have outstanding checked-out assets • Log the location of each asset • Log the time and date of each transaction
PS-13.1		Barcode client assets and created **media** (e.g., tapes, hard drives) upon receipt and store assets in the **vault** when not in use	• Apply dual barcodes to track assets (i.e., barcode on both the asset and the container/case) • Send assets directly to the **vault** after being bar-coded and return assets to the **vault** immediately when no longer needed
PS-13.2		Retain asset movement transaction logs for at least 90 days	• Store physical or digital logs for all asset movements; logs should include: – Barcode or unique ID of asset that was checked-in/checked-out – Time and date of check-in/check-out – Name and unique ID of the individual who checked out an asset – Reason for checkout – Location of asset

No.	Security Topic	Best Practice	Implementation Guidance
PS-13.3		Review logs from content **asset management** system and investigate anomalies	• Identify assets that have not been returned by the expected return date • Follow up with individuals who last checked out assets that are missing • Implement disciplinary procedures for individuals who do not follow **asset management** policies • Consider implementing automated notification when assets are checked out for extended periods of time
PS-13.4		Use studio AKAs (“aliases”) when applicable in asset tracking systems and on any physical assets	• Restrict knowledge of studio AKAs to personnel involved in processing client assets • Consider removing studio name on physical assets when appropriate
PS-14.0	Inventory Counts	Perform a quarterly inventory count of each client's pre-release project(s), reconcile against **asset management** records, and immediately communicate variances to clients	
PS-14.1		Segregate duties between the **vault** staff and individuals who are responsible for performing inventory counts	• Assign non-**vault** staff personnel to do random checks of count results
PS-14.2		Implement and review a daily aging report to identify highly sensitive assets that are checked out from the **vault** and not checked back in	• Perform daily aging reports either manually or through an **asset management** system • Investigate all exceptions
PS-15.0	Blank Media/ Raw Stock Tracking	Tag (e.g., barcode, assign unique identifier) blank stock/raw stock per unit when received	• Do not allow blank or raw **media** stock in secured production areas unless it is required for production purposes
PS-15.1		Store blank **media**/raw stock in a secured location	• Require access controls (e.g., locked cabinet, safe) to prevent unauthorized access • Restrict access to blank **media**/raw stock to personnel responsible for output creation • Require individuals to present a proper work order request to check out blank **media**/raw stock

No.	Security Topic	Best Practice	Implementation Guidance
PS-16.0	Client Assets	Restrict access to finished client assets to personnel responsible for tracking and managing assets	• Restrict access to only the **vault** staff, who can then authorize individuals to check out client assets when presented with a valid work order request • Segregate duties so that no member of the **vault** staff handles production data for processing
PS-16.1		Store client assets in a restricted and secure area (e.g., **vault**, safe)	• Implement an additional safe or high-security cage within the **vault** for highly sensitive titles
PS-17.0	Production Systems	Restrict access to production systems to appropriate personnel only	• Identify which roles require access to production systems and reconcile **access rights** quarterly
PS-18.0	Disposals	Require that rejected, damaged, and obsolete stock are erased, degaussed, shredded, or physically destroyed before disposal (e.g., DVD shredding, hard drive destruction) and update **asset management** records to reflect destruction	• Implement processes to inventory and reconcile stock, and then securely recycle or destroy rejected, damaged, and obsolete stock
PS-18.1		Follow the Department of Defense (DoD) sanitization standards for digital shredding and wiping	• Reference DoD 5220.22-M for digital shredding and wiping standards
PS-18.2		Store elements targeted for recycling/destruction in a secure location/container to prevent the copying and reuse of assets prior to disposal	• Establish and implement policies that limit the duration (e.g., 30 days) of storing rejected, damaged, and obsolete stock before recycling/destruction • Keep highly sensitive assets in secure areas (e.g., **vault**, safe) prior to recycling/destruction • Ensure that disposal bins are locked
PS-18.3		Maintain a log of asset disposal for at least 12 months	• Integrate the logging of asset disposal into the **asset management** process • Include a final disposal record for disposed assets in disposal logs

No.	Security Topic	Best Practice	Implementation Guidance
PS-18.4		Require third-party companies who handle destruction of content to provide a certificate of destruction for each completed job	• Consider requiring the following information on the certificate of destruction: – Date of destruction – Description of the asset destroyed/disposed of – Method of destruction – Name of individual who destroyed the assets
PS-18.5		Destroy check discs immediately after use	• Store and log check discs in a **vault** if the client requires vendors to keep them after use

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-19.0	Shipping	Require the facility to file a valid work/shipping order to authorize asset shipments out of the facility	• Include the following information on the work/shipping order: – Work/shipping order number – Name and company of individual who will pick up content – Time and date of pick up – Facility contact
PS-19.1		Track and log asset shipping details; at a minimum, include the following: • Time of shipment • Sender name and signature • Recipient name • Address of destination • Tracking number from courier • Reference to the corresponding work order	• Require recipient signature • Retain shipping logs for a minimum 90 days
PS-19.2		Validate assets leaving the facility against a valid work/shipping order	• Request valid identification from couriers and delivery personnel to authenticate individuals picking up shipments against the corresponding work order • Confirm that the shipped count matches the shipping documentation
PS-19.3		Secure assets that are waiting to be picked up	• Lock all doors and windows to shipping and receiving areas when unattended • Do not leave assets on desks unattended
PS-19.4		Prohibit couriers and delivery personnel from entering content/production areas of the facility	• Escort delivery personnel if access to content/production areas is necessary

No.	Security Topic	Best Practice	Implementation Guidance
PS-20.0	Receiving	Inspect delivered content upon receipt and compare to shipping documents (e.g., packing slip, manifest log)	• Identify and log any discrepancies (e.g., missing items, damaged **media**) • Report discrepancies to management, clients, and/or the sender immediately
PS-20.1		Maintain a receiving log to be filled out by designated personnel upon receipt of deliveries	• Record the following information: – Name and signature of courier/delivering entity – Name and signature of recipient – Time and date of receipt – Details of received asset
PS-20.2		Perform the following actions immediately: • Tag (e.g., barcode, assign unique identifier) received assets, • Input the asset into the **asset management** system • Move the asset to the restricted area (e.g., **vault**, safe)	• Store received assets that cannot be immediately tagged and vaulted in a secure **staging area** (e.g., high-security cage)
PS-20.3		Implement a secure method (e.g., secure drop box) for receiving overnight deliveries	• Ensure that schedules for expected items are only available to people who need to see them
PS-21.0	Labeling	Prohibit the use of title information, including AKAs ("aliases"), on the outside of packages	
PS-21.1		Include a return address that excludes the client or company name on all outgoing packages	
PS-22.0	Packaging	Ship all assets in closed/sealed containers, and use locked containers depending on asset value	• Do not use open bags or unpackaged tapes/DVDs by themselves • Apply restrictions to both hand-carried and courier-handled shipments

No.	Security Topic	Best Practice	Implementation Guidance
PS-22.1		Implement at least one of the following controls: • Tamper-evident tape • Tamper-evident packaging • Tamper-evident seals in the form of holograms • Secure containers (e.g., Pelican case with a combination lock)	• Establish and communicate a tampering procedure with common shipping partners, if applicable
PS-23.0	Transport Vehicles	Lock automobiles and trucks at all times, and do not place packages in visible auto/truck areas	

MANAGEMENT SYSTEM		PHYSICAL SECURITY			DIGITAL SECURITY		
ORGANIZATION AND MANAGEMENT	COMPETENCY	FACILITY	ASSET MANAGEMENT	TRANSPORT	INFRASTRUCTURE	CONTENT MANAGEMENT	CONTENT TRANSFER

No.	Security Topic	Best Practice	Implementation Guidance
DS-1.0	WAN	Segment **WAN(s)** by using stateful inspection **firewalls** with Access Control Lists that prevent unauthorized access to any internal network	• Configure **WAN firewalls** with Access Control Lists that deny all traffic to any internal network other than to explicit hosts that reside on the **DMZ** • Configure the **WAN** network to prohibit direct network access to the internal content/production network
DS-1.1		Develop a process to review **firewall Access Control Lists (ACLs)** to confirm configuration settings are appropriate and required by the business every 6 months	• Export **ACLs** from **firewalls** and/or **routers** • Review **ACLs** to confirm that network access is appropriate • Require management sign-off of review • Update **ACLs** accordingly
DS-1.2		Deny all protocols by default and enable only specific permitted secure protocols on the **WAN**	• Restrict all unencrypted communication protocols such as **Telnet** and **FTP** • Replace unencrypted protocols with encrypted versions, such as **SFTP** and Secure Shell (SSH)
DS-1.3		Place externally accessible servers (e.g., **SFTP** server, web servers) within the **DMZ**	• Harden servers in the **DMZ** • Isolate servers in the **DMZ** to provide only one type of service per server (e.g., **SFTP**, web server, etc.) • Implement **ACLs** to restrict access to the internal network from the **DMZ**
DS-1.4		Implement a process to patch network infrastructure devices (e.g., **firewalls**, **routers**, **switches**, etc.) regularly	• Implement a process to identify, evaluate and test patches for network infrastructure devices • Update network infrastructure devices to patch levels that address significant security vulnerabilities
DS-1.5		Harden network infrastructure devices based on security configuration standards	• Refer to the following security hardening standards for hardening network infrastructure devices: – NIST – SANS – NSA – CIS

No.	Security Topic	Best Practice	Implementation Guidance
DS-1.6		Do not allow remote access to **WAN** network infrastructure devices that control access to content	
DS-1.7		Secure backups of network infrastructure devices to a centrally secured server on the internal network	• Configure network infrastructure devices to store backups of configuration files to a secured location on the internal network • Ensure that only authorized administrators have access to the secured location • Ensure that restrictions are in place to mitigate brute-force attacks and unauthorized access to the configuration files if Trivial File Transfer Protocol (TFTP) is used for backups
DS-1.8		Perform an annual vulnerability scan on hosts that are externally accessible and remediate issues	• Implement a process to regularly scan for vulnerabilities for hosts that reside on the external network (e.g., **DMZ**)
DS-1.9		Ensure that after opening a fiber connection through a telecom service provider, the connection is terminated after the session ends	
DS-1.10		Allow only authorized personnel to request the establishment of a connection with the telecom service provider	

No.	Security Topic	Best Practice	Implementation Guidance
DS-2.0	Internet	Prohibit Internet access on systems (desktops/ servers) that process or store digital content	• Implement **firewall rules** to deny all outbound traffic by default and explicitly allow specific systems and ports that require outbound transmission to designated internal networks, such as antivirus definition servers, patching servers, etc. • Handle exceptions using an Internet gateway system (e.g., Citrix, Terminal Services, VNC, etc.) with the following controls: – The system is tightly controlled where web browsing is the only function of the server – Access to restricted sites is prohibited, including web-based e-mail sites, peer-to-peer, digital lockers, and other known malicious sites – Restrict content from being transferred to or from the system – Patch and update the system regularly with the latest virus definitions – Review system activity regularly
DS-2.1		Implement e-mail filtering software or appliances that block the following from **non-production networks**: • Potential phishing e-mails • Prohibited file attachments (e.g., Visual Basic scripts, executables, etc.) • File size restrictions limited to 10 MB	• Identify restricted content types for e-mail attachments and e-mail message body • Implement an e-mail filtering solution and configure based on restricted content types
DS-2.2		Implement web filtering software or appliances that restrict access to websites known for peer-to-peer file trading, viruses, hacking or other malicious sites	• Implement web-filtering/proxy server software to detect and prevent access to malicious websites

No.	Security Topic	Best Practice	Implementation Guidance
DS-3.0	LAN	Isolate the **content/production network** from **non-production networks** (e.g., office network, **DMZ**, etc.) by means of physical or logical network segmentation	• Define Access Control Lists that explicitly allow access to the **content/production network** from specific hosts that require access (e.g., antivirus server, patch management server, content delivery server, etc.) • Include explicitly defined ports and services that should allow access in the **Access Control Lists** • Segment or segregate networks based on defined security zones • Implement **firewall rules** to deny all outbound traffic by default and explicitly allow specific systems and ports that require outbound transmission to designated internal networks, such as antivirus definition servers, patching servers, etc. • Refer to DS-3.0 for guidance on accessing the Internet on the production environment • Assign **static IP addresses** by MAC address on **switches** • Disable **DHCP** on the **content/production network**
DS-3.1		Restrict access to the content/production systems to authorized personnel	
DS-3.2		Restrict remote access to the **content/production network** to only approved personnel who require access to perform their job responsibilities	• Maintain a list of **company personnel** who are allowed remote access to the **content/production network** • Develop processes to review activity on systems that reside on the **content/production network** • Configure remote access systems to use individual accounts • Limit remote access to a single method with Access Control Lists
DS-3.3		Disable all unused **switch** ports on the **content/production network** to prevent packet sniffing by unauthorized devices	• Connect to the device console and update configuration files to disable unused **switch** ports
DS-3.4		Restrict the use of non-switched devices such as hubs and repeaters on the **content/production network**	• Replace all hubs/repeats with **switches** or layer 3 devices

No.	Security Topic	Best Practice	Implementation Guidance
DS-3.5		Prohibit dual-homed networking (network bridging) on computer systems within the **content/production network**	• Implement network bridging at the network layer (e.g., **routers**, **firewalls**, **switches**, etc.) instead of using multiple NICs in one computer system
DS-3.6		Implement a network-based intrusion detection or prevention system on the **content/production network**	• Configure the network-based intrusion detection or prevention system to alert on or prevent suspicious network activity • Update attack signature definitions/policies regularly • Implement host-based intrusion detection system software on all workstations
DS-4.0	Wireless	Prohibit wireless networking and the use of wireless devices on the **content/production network**	• Restrict wireless guest networks to access only the Internet and not the **content/production network**
DS-4.1		Configure wireless networks on the **non-production network** with strong security controls: • Disable SSID broadcasting • Disable WEP • Enable **AES encryption** • Enable IEEE 802.1X or IEEE 802.11i where the option is available • Use RADIUS for authentication where the option is available Implement the following controls if pre-shared keys must be used: • Configure WPA2 with CCMP (**AES**) **encryption** • Set a complex passphrase (See DS-8.1 for passphrase complexity recommendations) • Change the passphrase periodically and when key **company personnel** terminate their employment • Enable **MAC address filtering**	• Implement an 802.1X framework for wireless networking, which includes the following: – Remote Access Dial In User Service (RADIUS) for Authentication, Authorization and Accounting – Lightweight Directory Access Protocol (LDAP) server, such as Active Directory, to manage user accounts – Public Key Infrastructure to generate and manage client and server certificates

No.	Security Topic	Best Practice	Implementation Guidance
DS-4.2		Implement a process to scan for rogue wireless access points annually	• Implement a process to roam and scan the facility for unprotected wireless access points • Configure a centralized wireless access solution (i.e., wireless controller) to alert administrators of rogue wireless access points upon detection, if possible
DS-4.3		Reduce the transmission power of the wireless access points to provide wireless networking to a limited coverage area	• Configure the wireless access point/controller to broadcast only within the required range
DS-5.0	I/O Device Security	Designate specific systems to be used for content input/output (I/O)	• Implement **ACLs** to allow traffic between the **content/production network** and systems used for I/O for specific source/destination **IP addresses**
DS-5.1		Block input/output (I/O) devices (e.g., **USB**, **FireWire**, e-SATA, **SCSI**, etc.) on all systems that handle or store content, with the exception of systems used for content I/O	• Consider the following for blocking **I/O devices**: – Change the registry setting to restrict write access to **I/O devices** for MS Windows-based systems – Remove the mass storage file to control write access on production stations for Mac-based systems – Disable **I/O devices** using group policy for systems using Microsoft Active Directory or Apple Open Directory – Use I/O port monitoring software to detect port usage if blocking output devices is not feasible
DS-5.2		Restrict the installation and/or use of **media** burners (e.g., DVD, Blu-ray, CD burners) and other devices with output capabilities to specific I/O systems used for outputting content to physical **media**	• Consider restricting write privileges using Group Policy
DS-5.3		Implement **AES** 128-bit **encryption** on hard drives and **USB** flash memory used to transport content	• Consider purchasing pre-encrypted drives (e.g., Rocstor Rocsafe, LaCie Rugged Safe)

No.	Security Topic	Best Practice	Implementation Guidance
DS-5.4		Prohibit the use of digital recording devices (e.g., smart phones, digital cameras, camcorders) in areas where sensitive content is accessible electronically	• Establish and implement policies prohibiting **company personnel** and **third party workers** from bringing digital recording devices into the content/content/production areas • Enforce disciplinary policies if **company personnel** are caught breaching policy • Use tamper-evident stickers on digital recording devices to prevent the use of cameras
DS-6.0	System Security	Install anti-virus software on all workstations and servers	• Install an enterprise anti-virus solution with a centralized management console
DS-6.1		Update anti-virus definitions daily	• Configure the centralized anti-virus management console to download and push definition updates at least once each day
DS-6.2		Scan file-based content for viruses prior to ingest onto the **content/production network**	• Perform scans on a system that is not connected to the **content/production network**
DS-6.3		Document and implement a strategy for performing virus scans such as: • Enable regular full system virus scanning on all workstations • Enable full system virus scans for servers, where applicable (e.g., non-SAN systems)	• Configure antivirus software to conduct a full system scan based upon the antivirus strategy • Configure antivirus software to execute during idle periods
DS-6.4		Implement a patch management process to regularly update patches (e.g., system, database, application, network devices) that remediate security vulnerabilities	• Where possible, implement a centralized patch management tool (e.g., WSUS, Shavlik, Altiris) to automatically deploy patches to all systems • Seek out patches from vendors and other third parties • Test patches prior to deployment • Implement an exception process and compensating controls for cases where there is a legitimate business case for not patching systems
DS-6.5		Prohibit users from being Administrators on their own workstations	• Ensure that the user account used to login to the workstation does not have privileges as an Administrator of the system

No.	Security Topic	Best Practice	Implementation Guidance
DS-6.6		Use cable locks on portable computing devices that handle content (e.g., laptops, tablets, towers) when they are left unattended	• Secure cable lock to a stationary object (e.g., table)
DS-6.7		Install remote-kill software on all portable computing devices that handle content to allow remote wiping of hard drives and other storage devices	• Encrypt all portable computing storage devices where possible
DS-6.8		Restrict software installation privileges to system administrators	• Prohibit the installation of unapproved software
DS-6.9		Require that legitimate licenses are used for all software and other proprietary software assets	• Develop processes to identify, track, and inventory software licenses • Prohibit the unauthorized installation of software requiring a license • Where possible, implement a software **asset management** system that identifies, tracks, and inventories software licenses
DS-6.10		Implement security baselines and standards to configure systems (e.g., laptops, workstations, servers) that are set up internally	• Develop a secure standard build that is used to image all systems
DS-6.11		Unnecessary services and applications should be uninstalled from content transfer servers	• Review the list of installed services (e.g. services.msc) on all content transfer servers and uninstall or disable any which are not required • Review the list of installed applications on all content transfer servers and uninstall any which are not required • Review the list of startup applications to ensure all non-essential applications are not running

No.	Security Topic	Best Practice	Implementation Guidance
DS-7.0	Account Management	Establish and implement an account management process for administrator, user, and service accounts for all **information systems** and applications that handle content	• Document policies and procedures for account management which address the following: – New user requests – User access modifications – Disabling and enabling of user accounts – User termination – Account expiration – Leaves of Absence
DS-7.1		Maintain traceable evidence of the account management activities (e.g., approval e-mails, change request forms)	• Retain evidence of management approvals and associated actions for all account management activities, where possible
DS-7.2		Assign unique credentials on a need-to-know basis using the principles of least privilege	• Assign credentials on a need-to-know basis for the following **information systems**, at a minimum: – Production systems – Content management tools – Content **transfer tools** – Network infrastructure devices – Logging and monitoring systems – Client web portal – Account management systems (e.g., Active Directory, NIS+)
DS-7.3		Restrict the use of service accounts to only applications that require them	• Prohibit users from using service accounts • Implement access control lists that restrict unauthorized use of service accounts
DS-7.4		Rename the default administrator accounts and limit the use of these accounts to special situations that require these credentials (e.g., operating system updates, patch installations, software updates)	• Consult the documentation for all hardware and software to identify all of the default account(s) • Change the password for all default accounts • Where possible, change the user name for each account • Disable administrator accounts when not in use

No.	Security Topic	Best Practice	Implementation Guidance
DS-7.5		Segregate duties to ensure that individuals responsible for assigning access to **information systems** are not themselves end users of those systems (i.e., personnel should not be able to assign access to themselves)	• Leverage an independent team to grant access to **information systems** when possible • Implement compensating controls when segregation is unattainable, such as: – Monitor the activity of **company personnel** and **third party workers** – Retain and review audit logs – Implement physical segregation – Enforce management supervision
DS-7.6		Monitor and audit administrator and service account activities	• Enable monitoring controls for systems and applications which support logging • Configure systems and applications to log administrator actions and record, at the minimum, the following information: – User name – Time stamp – Action – Additional information (action parameters) • Monitor service accounts to ensure that they are used for intended purposes only (e.g., database queries, application-to-application communication) • Implement a monthly process to review administrator and service account activity to identify unusual or suspicious behavior and investigate possible misuse
DS-7.7		Implement a process to review user access for all **information systems** that handle content and remove any user accounts that no longer require access quarterly	• Remove **access rights** to **information systems** from users that no longer require access due to a change in job role or termination of **company personnel** and/or **third party workers** • Remove or disable accounts that have not been used in over 90 days
DS-7.8		Review user access to content on a per-project basis	• Remove **access rights** to **information systems** from users that no longer require access due to project completion

No.	Security Topic	Best Practice	Implementation Guidance
DS-7.9		Disable or remove local accounts on systems that handle content	• Implement a centralized account management server (i.e., directory server such as LDAP or Active Directory) to authenticate user access to **information systems** • For network infrastructure devices, implement Authentication, Authorization, and Accounting (AAA) for account management
DS-8.0	Authentication	Enforce the use of **unique usernames** and passwords to access **information systems**	• Establish policies to enforce the use of **unique usernames** and passwords for all **information systems** • Configure **information systems** to require authentication, using **unique usernames** and passwords at a minimum
DS-8.1		Enforce a strong password policy for gaining access to **information systems**	• Create a password policy that consists of the following: – Minimum password length of 8 characters – Minimum of 3 of the following parameters: upper case, lower case, numeric, and special characters – Maximum password age of 90 days – Minimum password age of 1 day – Maximum invalid logon attempts of between 3 and 5 attempts – Password history of ten previous passwords
DS-8.2		Implement two-factor authentication (e.g., username/password and hard token) for remote access (e.g., **VPN**) to the network	• Require individuals to provide two of the following for remote access: – Information that the individual knows (e.g., password, PIN number) – A unique physical item that the individual has (e.g., token, **keycard**) – A unique physical quality that is unique to the individual (e.g., fingerprint, retina)
DS-8.3		Implement password-protected screensavers for servers and workstations	• Configure servers and workstations manually or via a policy (such as Active Directory group policies) to activate a password-protected screensaver after a maximum of 10 minutes of inactivity

No.	Security Topic	Best Practice	Implementation Guidance
DS-9.0	Logging and Monitoring	Implement real-time logging and reporting systems to record and report security events; gather the following information at a minimum: • When (time stamp) • Where (source) • Who (user name) • What (content)	• Enable logging on the following infrastructure systems and devices at a minimum: – Infrastructure components (e.g., **firewalls**, authentication servers, network operating systems, remote access mechanisms) – Production operating systems – Content management components (e.g., storage devices, content servers, content storage tools, content transport tools) – Systems with Internet access – Consider implementing a server to manage the logs in a central repository (e.g., syslog/log management server, Security Information and Event Management (SIEM) tool)
DS-9.1		Configure logging systems to send automatic notifications when security events are detected in order to facilitate active response to incidents	• Define events that require investigation and enable automated notification mechanisms to appropriate personnel; consider the following: – Successful and unsuccessful attempts to connect to the **content/production network** – Unusual file size and/or time of day transport of content – Repeated attempts for unauthorized file access
DS-9.2		Investigate any unusual activity reported by the logging and reporting systems	• Incorporate **incident response** procedures for handling detected security events
DS-9.3		Review logs weekly	• Investigate any unusual activity that may indicate a serious security incident • Identify any additional unusual events that are not currently being alerted on and configure the logging and reporting system to send alerts on these events • Correlate logs from different systems to identify patterns of unusual activity

No.	Security Topic	Best Practice	Implementation Guidance
DS-9.4		Enable logging on content transfers and include the following information at a minimum: • Username • Timestamp • File name • Source **IP address** • Destination **IP address** • Event (e.g., download, view)	
DS-9.5		Retain logs for at least 6 months	• Seek guidance from legal counsel to determine any regulatory requirements for log retention • Store content logs on a centralized server that can be accessed only by specific users and is secured in an access-controlled room
DS-9.6		Restrict log access to appropriate personnel	• Maintain Access Control Lists to ensure that only personnel responsible for log monitoring and review have permission to view logs • Segregate duties to ensure that individuals are not responsible for monitoring their own activity • Protect logs from unauthorized deletion or modification by applying appropriate **access rights** on log files
DS-9.7		Send automatic notifications to the production coordinator(s) upon outbound content transmission	• Configure the content transfer system to send a notification (e.g. an e-mail) to the production coordinator(s) each time a users sends content out of the internal network

MANAGEMENT SYSTEM		PHYSICAL SECURITY			DIGITAL SECURITY		
ORGANIZATION AND MANAGEMENT	COMPETENCY	FACILITY	ASSET MANAGEMENT	TRANSPORT	INFRASTRUCTURE	CONTENT MANAGEMENT	CONTENT TRANSFER

No.	Security Topic	Best Practice	Implementation Guidance
DS-10.0	Security Techniques	Ensure that security techniques (e.g., spoiling, invisible/visible **watermarking**) are available for use and are applied when instructed	
DS-10.1		Encrypt content on hard drives using **AES** 128-bit **encryption** by either: • File-based **encryption**: (i.e., encrypting the content itself) • Drive-based **encryption**: (i.e., encrypting the hard drive)	• Implement one or more of the following: – File-based **encryption** such as encrypted DMGs or encrypted ZIP files – Drive-based **encryption** using software such as TrueCrypt
DS-10.2		Send decryption keys or passwords using an out-of-band communication protocol (i.e., not on the same storage **media** as the content itself)	• Send decryption keys or passwords using a different method than that which was used for the content transfer • Check to ensure key names and passwords are not related to the project or content

MANAGEMENT SYSTEM		PHYSICAL SECURITY			DIGITAL SECURITY		
ORGANIZATION AND MANAGEMENT	COMPETENCY	FACILITY	ASSET MANAGEMENT	TRANSPORT	INFRASTRUCTURE	CONTENT MANAGEMENT	CONTENT TRANSFER

No.	Security Topic	Best Practice	Implementation Guidance
DS-11.0	Transfer Tools	Implement **transfer tools** that use access controls, a minimum of **AES** 128-bit **encryption** and strong authentication for content transfer sessions	• Consider the following **transfer tools**: – Aspera – Signiant – WAM!NET – SmartJog – **Secure FTP**
DS-11.1		Implement an exception process, where client prior approval must be obtained in writing, to address situations where encrypted **transfer tools** are not used	• Require clients to sign off on exceptions where unencrypted **transfer tools** must be used • Document and archive all exceptions • Use randomly generated usernames and passwords that are securely communicated for authentication
DS-12.0	Transfer Device Methodology	Implement and use dedicated systems for content transfers	• Ensure editing stations and content storage servers are not used to directly transfer content
DS-12.1		Segment systems dedicated to transfer files from systems that store or process content and from the **non-production network**	• Segment systems on separate physical networks or logically separated **VLANs**
DS-12.2		Place content transfer systems in a **Demilitarized Zone** (**DMZ**) and not in the **content/production network**	• Harden content transfer systems prior to placing them in the **DMZ** • Implement **Access Control Lists (ACLs)** that restrict all ports other than those required by the content **transfer tool** • Implement **ACLs** to restrict traffic between the internal network and the **DMZ** to specific source/destination **IP addresses**

No.	Security Topic	Best Practice	Implementation Guidance
DS-12.3		Remove content from content transfer devices immediately after successful transmission/receipt	• Require clients to provide notification upon receipt of content • Implement a process to remove content from transfer devices • Where applicable, remove client access to **transfer tools** immediately after project completion
DS-13.0	Client Portal	Restrict access to web portals which are used for transferring content, streaming content and key distribution to authorized users	• Implement access control measure around web portals that transfer content, stream content and distribute keys by implementing one or more of the following: – Require user credentials – Integrate machine and/or user keys for authentication and authorization – Limit portal access to specific networks, **VLANs**, subnets, and/or **IP address** ranges – Restrict the ability to upload/download as applicable from the client portal
DS-13.1		Assign unique credentials (e.g., username and password) to portal users and distribute credentials to clients securely	• Do not embed user names and passwords in content links • Consider distributing the user credentials and content links in separate e-mails • Consider distributing user credentials via phone or SMS • Create a password policy that consists of the following: – Minimum password length of 8 characters – Minimum of 3 of the following parameters: upper case, lower case, numeric, and special characters – Maximum password age of 90 days – Minimum password age of 1 day – Maximum invalid logon attempts of between 3 and 5 attempts – Password history of ten previous passwords
DS-13.2		Ensure users only have access to their own **digital assets** (i.e., client A must not have access to client B's content)	• Implement a process to review file/directory permissions • Ensure that access is restricted to only those that require it

No.	Security Topic	Best Practice	Implementation Guidance
DS-13.3		Place the web portal on a dedicated server in the **DMZ** and limit access to/from specific **IPs** and protocols	• Implement **Access Control Lists (ACLs)** that restrict all ports other than those required by the client portal • Implement **ACLs** to restrict traffic between the internal network and the **DMZ** to specific source/destination **IP addresses**
DS-13.4		Use HTTPS and enforce use of a strong cipher suite (e.g.,SSLv3 or TLS v1) for the internal/external web portal	
DS-13.5		Do not use persistent cookies or cookies that store credentials in plaintext	• Review the use of cookies by existing web-based applications and ensure none of them store credentials in plaintext • If an application is storing credentials in plaintext cookies then take one of the following actions: – Reconfigure the application – Update the application – Request a security patch from the application developer
DS-13.6		Set access to content on internal or external portals to expire automatically at predefined intervals, where configurable	
DS-13.7		Restrict client portal access to originate from a specific **IP address** or range	
DS-13.8		Test for web application vulnerabilities annually	• Use industry accepted testing guidelines, such as those issued by the Open Web Application Security Project (OWASP) to identify common web application vulnerabilities such as Cross Site Scripting (XSS), SQL Injection, and Cross Site Request Forgery (CSRF) • See Appendix F for further information
DS-13.9		Allow only authorized personnel to request the establishment of a connection with the telecom service provider	

No.	Security Topic	Best Practice	Implementation Guidance
DS-13.10		Prohibit transmission of content using e-mail (including webmail) from the **non-production network**, and manage exceptions using the exception policy	• Consider the use of secure e-mail appliance servers (e.g., Cisco IronPort, Sophos E-Mail Security Appliance, Symantec PGP Universal Gateway Email)
DS-13.11		Review access to the client web portal at least quarterly	• Remove **access rights** to the client web portal once projects have been completed • Remove any inactive accounts

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. In the best practices guidelines, all terms that are included in this glossary are highlighted in **bold.**

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.
Advanced Encryption Standard (AES)	A NIST symmetric key encryption standard that uses 128-bit blocks and key lengths of 128, 192, or 256 bits.
Asset Management	The system by which assets are tracked throughout the workflow, from acquisition to disposal.
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.
Company Personnel	Any individual who works directly for the facility, including employees, temporary workers, and interns.

Term or Acronym	Description
Content/ Production Network	A computer network that is used to store, transfer, or process media content.
Digital Asset	Any form of content and/or media that have been formatted into a binary source which includes the right to use it.
Due Diligence	The research or investigation of a potential employee or third party worker that is performed before hire to ensure good standing.
Dynamic Host Configuration Protocol (DHCP)	Protocol used to automatically assign IP addresses to all nodes on the network.
Demilitarized Zone (DMZ)	Physical or logical sub-network that contains and exposes an organization's external services to a larger untrusted network, usually the Internet.
Encryption	The conversion of data into a form, called a ciphertext, which cannot be easily understood by unauthorized people.

Term or Acronym	Description
Fingerprinting	A 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.
FireWire	A high-speed interface that allows data to be transmitted from external devices to a computer.
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).
Incident Response	The detection, analysis, and remediation of security incidents.
Information Systems	Any electronic or computer-based system that is used by the facility to process information. Information systems include applications, network devices, servers, and workstations, among others.
I/O Device	Devices used to communicate with and/or between computers (e.g., USB and FireWire drives).
IP Address	A numerical identification (logical address) that is assigned to devices participating in a computer network.
Key Management	The creation, distribution, storage, and revocation of encryption keys that are used to access encrypted content.

Term or Acronym	Description
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 restrict access to a computer network.
Master Key	Keys that offer access to all doors (interior and exterior) at any given facility. Keys with access to all high security areas are also 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.
Non-Production Network	All computer networks that are not used for processing or transferring media content. Non-production networks can include the office or administrative network and the client network.
Risk Assessment	The identification and prioritization of risks that is performed to identify possible threats to a business.
Risk Management	The identification, analysis, and mitigation of risks through risk assessment and the implementation of security controls.
Router	Device whose software and hardware are tailored to the tasks of steering and forwarding information.

Term or Acronym	Description
Secure File Transfer Protocol (SFTP)	A TCP/IP protocol that is used to encrypt and transfer files across a network; an encrypted version of FTP.
Segregation of Duties	A security principle by which no single person should have the ability to complete a task on his own; a principle by which no single person should be responsible for more than one related function.
Small Computer System Interface (SCSI)	Standards for physically connecting and transferring data between computers and peripheral devices.
Staging Area	An area where content is stored prior to being picked up (e.g., for delivery or ingestion).
Static IP	Configuration wherein a computer uses the same IP address each time it powers up.
Switch	Computer networking device that connects multiple machines within a network and channels traffic to specific destinations.
Telnet	Network Protocol used on the Internet or local area network to access remote machines.
Third Party Worker	Any individual who works for an external company but is hired by the facility to provide services. Third party workers include contractors, freelancers, and temporary agencies.
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.

Term or Acronym	Description
Transfer Tools	Tools used for the electronic transmission of digital assets through a network, usually with acceptable encryption and authentication mechanisms.
Transfer Protocol	The procedure involved in transmitting files over a computer network or the Internet.
Trusted Device List (TDL)	A list of specific digital devices that are approved to playback content.
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.
Vault	An area that is dedicated to storing physical media with content.
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.
Workflow	The sequence of steps that a company performs on content.

APPENDIX B — MPAA TITLE AND DISTRIBUTION CHANNEL DEFINITIONS

Title Types

Title Type	Description
Feature	A type of work released theatrically or direct to home video or to Internet that includes the following types: **Feature Type** / **Description** Feature Film — A full length movie. Short — A film of length shorter than would be considered a feature film. Long-Form Non-Feature — Other works, for example, a documentary.
TV Episodic	A type of work that is TV, web or mobile related and includes episodes of a season or miniseries. A pilot is also an episode as are other specialized sequences (such as “webisode” or “mobisode”).
TV Non-Episodic	A type of work that is TV, web, or mobile related, but does not have episodes (e.g., made-for-television movies, sporting events, or news programs).
Promotion/Advertisement	A type of work that includes: • “Promotion” – Any promotional material associated with media. This includes teasers, trailers, electronic press kits and other materials. Promotion is a special case of ‘Ad’.

Title Type	Description
Ad	Any form of advertisement including TV commercials, infomercials, public service announcements and promotions not covered by “Promotion.” This does not include movie trailers and teasers even though they might be aired as a TV commercial.
Music	A type of work that includes ringtone, music videos and other music.
Other	A type of work that includes: **Type** / **Description** Excerpt — An asset that consists primarily of portion or portions of another work or works. Supplemental — Material designed to supplement another work. For example, an extra associated with a DVD. Collection — A collection of assets not falling into another category. For example, a collection of movies. Franchise — A collection or combination of other types, for example, a franchise might include multiple TV shows, or TV shows and movies.

Distribution Channels

Distribution Channel	Description
Theatrical	A feature film is released exclusively into theaters.
Non-Theatrical	A motion picture is released publicly in any manner other than television, home video or theatrical. It includes the exhibition of a motion picture (i) on airplanes, trains, ships and other common carriers, (ii) in schools, colleges and other educational institutions, libraries, governmental agencies, business and service organizations and clubs, churches and other religious oriented groups, museums, and film societies (including transmission of the exhibition by closed circuit within the immediate area of the origin of such exhibition), and (iii) in permanent or temporary military installations, shut-in institutions, prisons, retirement centers, offshore drilling rigs, logging camps, and remote forestry and construction camps (including transmission of the exhibition by closed circuit within the immediate area of the origin of such exhibition).
Home Video	A motion picture is released for sell-through and rental sales of packaged goods at the wholesale level, for example on DVD or Blu-Ray.
Free Television	A motion picture is released to the public on free broadcast airwaves, usually as set forth in the license agreement with networks, television stations, or basic cable networks.
Pay Television	A motion picture is released to the public in a manner that requires payment by at least one participant in the broadcast chain, such as video-on-demand, cable, satellite and pay-per-view.
Internet	A motion picture is released in any one of the following online distribution channels:

Type	Description
Electronic Sell-Through (EST) or Download to Own (DTO)	Permanent digital copies sold online.
Online Rental or Video-on-Demand (VOD)	Paid rentals online for temporary viewing.
Subscription Video-on-Demand (SVOD)	Online subscription rental viewing online.
Online Free Video-on-Demand (FVOD)	Free online streaming viewing usually supported by ad revenue.
Other	Online and new media such as mobile or Internet Protocol TV.

APPENDIX C — MAPPING OF 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 800-53 Reference
MS-1.0	Executive Security Awareness/ Oversight	4.1, 6.1.1	PM-1, PM-2
MS-1.1		6.1.1	AT-2, AT-3, PM-1, PM-2
MS-2.0	Risk Management	4.1	CA-1, RA-1
MS-2.1		7.2	RA-2
MS-2.2		4.1, 4.2	CA-2, CA-5, RA-3
MS-3.0	Security Organization	6.1.3	PM-2
MS-4.0	Budgeting		PM-3
MS-5.0	Policies and Procedures	5.1.1, 6.1.1	PL-1
MS-5.1		5.1.2	PL-1
MS-5.2		8.1.3	PL-1, PS-7
MS-6.0	Incident Response	13.1	IR-1, IR-8
MS-6.1			IR-2
MS-6.2		13.1.1	IR-6, IR-7
MS-6.3		13.1, 13.2.2	IR-4, IR-5
MS-7.0	Workflow	10.1	
MS-7.1		4.1, 4.2, 10.1	
MS-8.0	Segregation of Duties	10.1.3	AC-5

No.	Security Topic	ISO 27002 Reference	NIST 800-53 Reference
MS-9.0	Background Checks	8.1.2	PS-3
MS-10.0	Confidentiality Agreements	6.1.5	PL-4, PS-6, SA-9
MS-10.1		8.3.2, 8.3.3	PS-4
MS-11.0	Disciplinary Measures	8.2.3	PS-8
MS-12.0	Content Security and Piracy Awareness	8.2.2	AT-1, AT-2, AT-3, AT-4
MS-13.0	Third Party Use and Screening	6.1.5	PL-4, PS-6, SA-9
MS-13.1		6.2.3	PS-7, SA-9
MS-13.2		6.2, 10.2	PS-4
MS-13.3		6.2	
MS-13.4		6.2.3, 11.1, 11.2	PS-7
MS-13.5		6.2.3	
PS-1.0	Entry/Exit Points	9.1.1	PE-3
PS-1.1		9.1.2	PE-3, PE-6
PS-1.2		9.1.3	PE-3
PS-2.0	Visitor Entry/Exit	9.1.2	PE-8
PS-2.1		9.1.2	PE-7
PS-2.2		9.1.2	PE-3

No.	Security Topic	ISO 27002 Reference	NIST 800-53 Reference
PS-2.3		9.1.2	PE-7
PS-3.0	Identification	9.1.2	PE-3
PS-4.0	Perimeter Security	9.1.1	PE-3
PS-5.0	Emergency Protocol	9.1.2	PE-11
PS-5.1		9.1.2	CP-2, CP-3, CP-4, IR-2
PS-6.0	Alarms	9.1.1	PE-3, PE-6
PS-6.1			PE-6
PS-6.2		11.2.1	AC-6
PS-6.3		11.2.1, 11.2.2, 11.2.4	
PS-6.4		9.1.1	IR-2, IR-3
PS-6.5			PE-3
PS-7.0	Authorization	11.2	PE-1, PE-2, PE-3
PS-7.1		11.2.4	PE-2, PS-4, PS-5
PS-8.0	Electronic Access	9.1.2, 9.1.3	PE-2, PE-3
PS-8.1		11.2	PE-2, PE-3
PS-9.0	Keys	9.1.2, 9.1.3	PE-2, PE-3
PS-9.3		7.1.1	CM-8
PS-10.0	Cameras		PE-6
PS-10.2		9.1.2, 9.1.3	PE-6
PS-10.3			PE-6
PS-10.4		10.10.6	AU-8
PS-11.0	Logging and Monitoring	10.10.2, 10.10.3	AU-3, AU-6 AU-9, AU-11
PS-11.1		13.1	AU-6
PS-11.2		10.1	AU-6
PS-11.3		10.10.3	AU-9
PS-12.0	Searches	8.1.3	
PS-13.0	Inventory Tracking	7.1	CM-8
PS-13.1			MP-3
PS-13.2		10.10.3, 10.10.6, 15.1.3	AU-9, AU-11
PS-13.3			AU-6
PS-14.0	Inventory Counts	7.1.1	AU-6
PS-14.1		10.1.3	AC-5
PS-14.2			IR-4, IR-5
PS-15.0	Blank Media/ Raw Stock Tracking	7.1.1	MP-4
PS-15.1		7.1.1, 10.7.1	MP-4, PE-2, PE-3
PS-16.0	Client Assets	7.1.1, 10.7.1	MP-4, PE-2, PE-3
PS-16.1		7.1.1, 10.7.1 9.1.2	MP-2, MP-4
PS-17.0	Production Systems	9.1.2	PE-2
PS-18.0	Disposals	9.2.6, 10.7.2	MP-6
PS-18.2		9.2.6, 10.7.2	MP-6
PS-18.3			MP-6
PS-18.4			MP-6
PS-19.0	Shipping	10.8.2	MP-5
PS-19.1		10.8.2, 10.8.3	AU-11, PE-16
PS-19.2		10.8.2, 10.8.3	MP-5
PS-19.4		9.1.2	PE-3, PE-7

No.	Security Topic	ISO 27002 Reference	NIST 800-53 Reference
PS-20.0	Receiving	10.8.2, 10.8.3	PE-16
PS-20.1			MP-5
PS-20.2		7.1, 7.2	MP-3, MP-4
PS-22.0	Packaging	10.8.3	MP-5
PS-22.1		10.8.3	
DS-1.0	WAN	11.4	AC-3
DS-1.1		11.1.1	AC-2
DS-1.2		11.4	CM-7
DS-1.3		11.4.2, 11.4.5, 11.6.2	AC-20, CA-3, SC-7
DS-1.6		11.4.2	AC-6, AC-17
DS-1.7		10.5.1	
DS-1.8		12.6.1	RA-3, RA-5
DS-2.0	Internet	11.2.2	CA-3
DS-2.1		7.1.3	PL-4
DS-2.2		7.1.3	AC-6, PL-4
DS-3.0	LAN	11.4.5, 11.6.2	SC-7
DS-3.1		11.2	
DS-3.2		11.4.2	AC-6, AC-17
DS-3.3		11.4.4	CM-7
DS-3.6		10.6.2, 10.10	SI-4
DS-4.0	Wireless	10.6.1	AC-18
DS-4.1		10.6.1	AC-18
DS-4.2		12.6	SI-4
DS-4.3			AC-18
DS-5.1		10.7.1, 10.10.2	AC-19, MP-2
DS-5.2			PE-5
DS-5.3			AC-19, SC-13
DS-5.4		7.1.3, 9.1.5	AC-19
DS-6.0	System Security	10.4.1	SI-3
DS-6.1		10.4.1	SI-3
DS-6.2		10.4.1	SI-3
DS-6.3		10.4.1	SI-3
DS-6.4		12.5	SI-2, RA-5
DS-6.5		10.1.3	AC-5, SC-2
DS-6.6		11.3.2	PE-3
DS-6.8		12.4.1	SA-7
DS-6.9		10.8.2, 15.1.2	SA-6
DS-6.10			CM-1, CM-2
DS-6.11		11.4.4	AC-3, AC-6
DS-7.0	Account Management	11.2	AC-2
DS-7.1		11.2.1	AC-2
DS-7.2		11.2.2	AC-2, AC-6, IA-4
DS-7.5		10.1.3	AC-5
DS-7.6		10.10.4	AU-2, AU-12
DS-7.7		11.2.4	PS-4, PS-5
DS-7.8		11.2.4	AC-2, PE-2
DS-7.9			AC-2
DS-8.0	Authentication	11.2.1, 11.5.2	IA-2, IA-4
DS-8.1		11.2.3	AC-7, IA-5
DS-8.2		11.4.2, 11.5.2	AC-17
DS-8.3		11.3.2, 11.3.3	AC-11

No.	Security Topic	ISO 27002 Reference	NIST 800-53 Reference
DS-9.0	Logging and Monitoring	10.1	SI-4, AU-2, AU-3
DS-9.1		10.10.2, 10.10.5	AU-1, AU-6
DS-9.2		10.10.5	AU-1, AU-6
DS-9.3		10.10.2, 10.10.5	AU-1, AU-6
DS-9.4		10.1	AU-2, AU-3
DS-9.5			AU-11
DS-9.6		10.1.3, 10.10.3	AU-9
DS-10.0	Security Techniques	7.2.2	
DS-10.1		12.3.1	IA-5, SC-13
DS-10.2		12.3.2	SC-9, SC-12
DS-11.0	Transfer Tools	12.3.1	IA-5, SC-13
DS-12.0	Transfer Device Methodology	10.8	
DS-12.1		11.4.5	AC-4, SC-7
DS-12.2		11.4.5	AC-4, AC-20, SC-7
DS-12.3		10.7.1	MP-6
DS-13.0	Client Portal	11.6.1	AC-6
DS-13.1		11.4.2, 11.5.3	IA-5
DS-13.2		11.2.2	AC-2, AC-3, AC-6
DS-13.3		11.4.5	AC-4, AC-20
DS-13.4		11.4.7	
DS-13.6		11.3.2	SC-10
DS-13.7		11.4.7	AC-4
DS-13.8		12.6.1	RA-3, RA-5
DS-13.9			AC-6
DS-13.11		11.2.4	AC-2

APPENDIX D — 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.

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

   Facilities should always apply the more restrictive set of supplemental best practices unless the work process are separated from each other, in which case, you should only apply the supplemental best practices to the environment for that service.

3. **Is my facility required to apply all items included in the "Implementation Guidance" section of the best practices?**

   No. Information contained in this section of the guidelines is intended to assist you in determining the best way to structure a particular security control. If your facility has a site survey conducted by the MPAA, our assessment will only compare your facility's practices against the respective best practice section of the guidelines at a given point in time. (For more information about how to receive an MPAA site survey, you can contact us at sitesurvey@mpaa.org.)

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

   Please contact the respective systems vendor in order to identify possible solutions to enable systems to follow best practices. Solutions can include patching, updating the version or even changing to a more secure system. Alternative security measures can also be used if technical limitations prevent the implementation of best practices; however, these are normally not considered to cover the associated risks. Exceptions to the implementation of security guidelines due to system limitations should be formally documented and approved by your clients.

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

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

APPENDIX E — SUGGESTED POLICIES AND PROCEDURES

Below are some common areas for which security policies and procedures should be developed and implemented in order to safeguard 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
   - Shipping protocols
   - Inventory storage on-site, during transport
3. **Information Technology Security**
   - Internet usage policy
   - Authentication and authorization
   - Password policy
   - Malicious code protection/anti-virus
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 (SOD)
   - 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 (NDAs)
6. **Incident Response**
   - Incident identification and analysis
   - Incident escalation and reporting
   - Incident response processes and procedures
   - Post mortem review procedures and lessons learned

APPENDIX F — OTHER RESOURCES AND REFERENCES

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

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

International Organization for Standardization (ISO), Standard 27005. *Information technology - Security technique- Information security risk management*. June 2008.http://www.27000.org/iso-27005.htm

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

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

SysAdmin, Audit, Networking, and Security (SANS Institute). *Glossary of Terms Used in Security and Intrusion Detection* http://www.sans.org/resources/glossary.php#m

The Open Web Application Security Project (OWASP) – Testing Guide http://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf

National Institute of Standards and Technology Special Publication 800-88. *Guidelines for Media Sanitization*, September 2006. http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

National Industrial Security Program - Operating Manual (DoD 5220.22-M), February 2006 http://www.dss.mil/isp/odaa/documents/nispom2006-5220.pdf

The Center for Internet Security – Security Benchmarks http://cisecurity.org/en-us/?route=downloads.multiform

National Security Agency - Security Configuration Guides http://www.nsa.gov/ia/guidance/security_configuration_guides/

National Institute of Standards and Technology Special Publication 800-92. *Guide to Computer Security Log Management,* September 2006. http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

National Institute of Standards and Technology Special Publication 800-44. *Guidelines on Securing Public Web Servers,* September 2007. http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf

National Institute of Standards and Technology Special Publication 800-40. *Creating a Patch and Vulnerability Management Program,* November 2005. http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf

APPENDIX G — REPORTING PIRACY TO THE MPAA

MPAA Report Piracy Online

You can report piracy directly to the MPAA:

http://www.mpaa.org/contentprotection/report-piracy

MPAA and MPA 24-Hour Piracy Tip Lines

The following list presents the 24-hour tip line contact information for each country where the MPAA works with a local content protection office:

North America and Latin America Region	
Canada, French and English	(800) 363-9166
United States	(800) 371-9884
Europe, Middle East, Africa (EMEA) Region	
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

Asia Pacific (APAC) Region	
Australia	+61 29997 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

A complete listing of general contact information for all content protection regional and country offices is located at: www.mpaa.org/about/around-the-world

MPAA Online Resources

Additional information about the MPAA can also be found on this website located at: www.mpaa.org

You can also learn about programs worldwide to protect content during the exhibition at: www.fightfilmtheft.org

End of Document