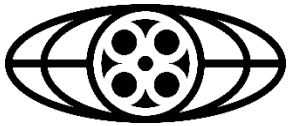


MOTION PICTURE ASSOCIATION

MPA Content Security Program

CONTENT SECURITY BEST PRACTICES
COMMON GUIDELINES

https://www.motionpictures.org/best-practices

Version 4.06

October 25, 2019

DOCUMENT HISTORY

Version	Date	Description	Author
1.0	December 31, 2009	Initial Public Release	Deloitte & Touche LLP, MPA, MPA Member Companies
2.0	May 15, 2011	Updates and Revisions Consolidation into Common Guidelines and Supplementals	PwC LLP, MPA, MPA Member Companies
2.1	January 1, 2013	Updates and Revisions	PwC LLP, MPA, MPA Member Companies
3.0	April 2, 2015	Updates and Revisions	MPA, MPA Member Companies
4.02	December 1, 2017	Updates and Revisions	MPA, MPA Member Companies
4.03	July 18, 2018	Updates and Revisions	MPA, MPA Member Companies
4.04	October 12, 2018	Updates and Revisions	MPA Content Security, MPA IT, MPA Member Companies
4.05	May 31, 2019	Updates and Revisions	MPA Content Security, MPA Member Companies
4.06	October 25. 2019	Updates and Revisions	MPA Content Security, MPA Member Companies

Summary of Changes Made to this Version:			
Version	**Date**	**Description**	**Comments**
4.06	October 25. 2019	1. Rebranding the entire document, changing MPAA to MPA and replacing the logo 2. Addition of a Change log 3. Changes to the following Best Practices: MS-6.0, MS-11.0, MS-11.1, PS-9.0, PS-9.2, PS-9.3, DS-8.1, DS-8.2.1, DS-15.1, DS-15.5, 4. Additions to the glossary as follows: IP Camera, MFA, NVR, Penetration Testing, PAM, Service Account, Vulnerability Scans 5. Update of Appendix C , DS-8.1 NIST Reference	This revision primarily focused on changes in the following areas: 1. Updating references to CCTV to include best practices for IP based cameras. 2. Updating the password policy to consider the latest standards from NIST 800-63b, services accounts, and MFA 3. Updating glossary items A more detailed change log of each individual change is available from the MPA upon request

TABLE OF CONTENTS

I. Best Practices Overview

Introduction

For more than three decades, the Motion Picture Association (MPA) has managed content security assessments on behalf of its Member Companies (Members): Paramount Pictures Corporation; Sony Pictures Entertainment Inc.; Universal City Studios LLC; Netflix; Walt Disney Studios Motion Pictures and Warner Bros. Entertainment Inc. Fox Studios (a former member) was bought by Disney in 2019 and Netflix joined in 2019.

Starting in 2007, these reviews were performed using a standardized survey model, process and report template. Since then, almost 500 facilities have been surveyed in 32 countries.

During the middle of 2018, the MPA started performing assessments through the TPN (Trusted Partner Network). The MPA is also involved in the governance and operations of the TPN program.

The MPA 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 MPA Content 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 the following:

- 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 assessment vehicle for further individual discussions regarding content security between Members 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: contentsecurity@motionpictures.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 DiscQC	• Clean – Full Feature	• Pre-Home Video
8	**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
9	**Post-Production Services**	• Telecine • Duplication • Editing • Finishing • QC	• High-Resolution – Full or Partial Content	• Pre-Theatrical • Pre-Home Video • Catalog
10	**Replication**	• Pre-Mastering • Mastering • Replication • Check Disc Creation	• High Resolution • Clean Image	• Pre-Home Video
11	**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)
12	**Application**	• Application Development	• Varied	• Varied
13	**Cloud**	• Hosting • Data Center	• Varied	• Varied

III. Risk Management and Document Organization

Risk Assessment

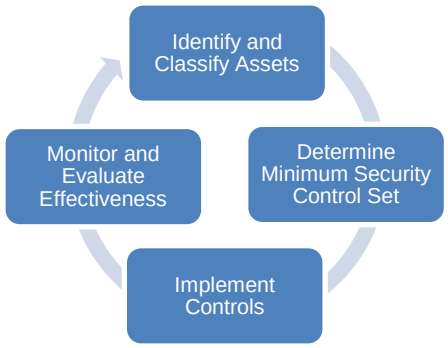
Risks should be identified through a risk assessment, and appropriate controls should be implemented to decrease risk to an acceptable level and ensure that business objectives are met.

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 breach 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.

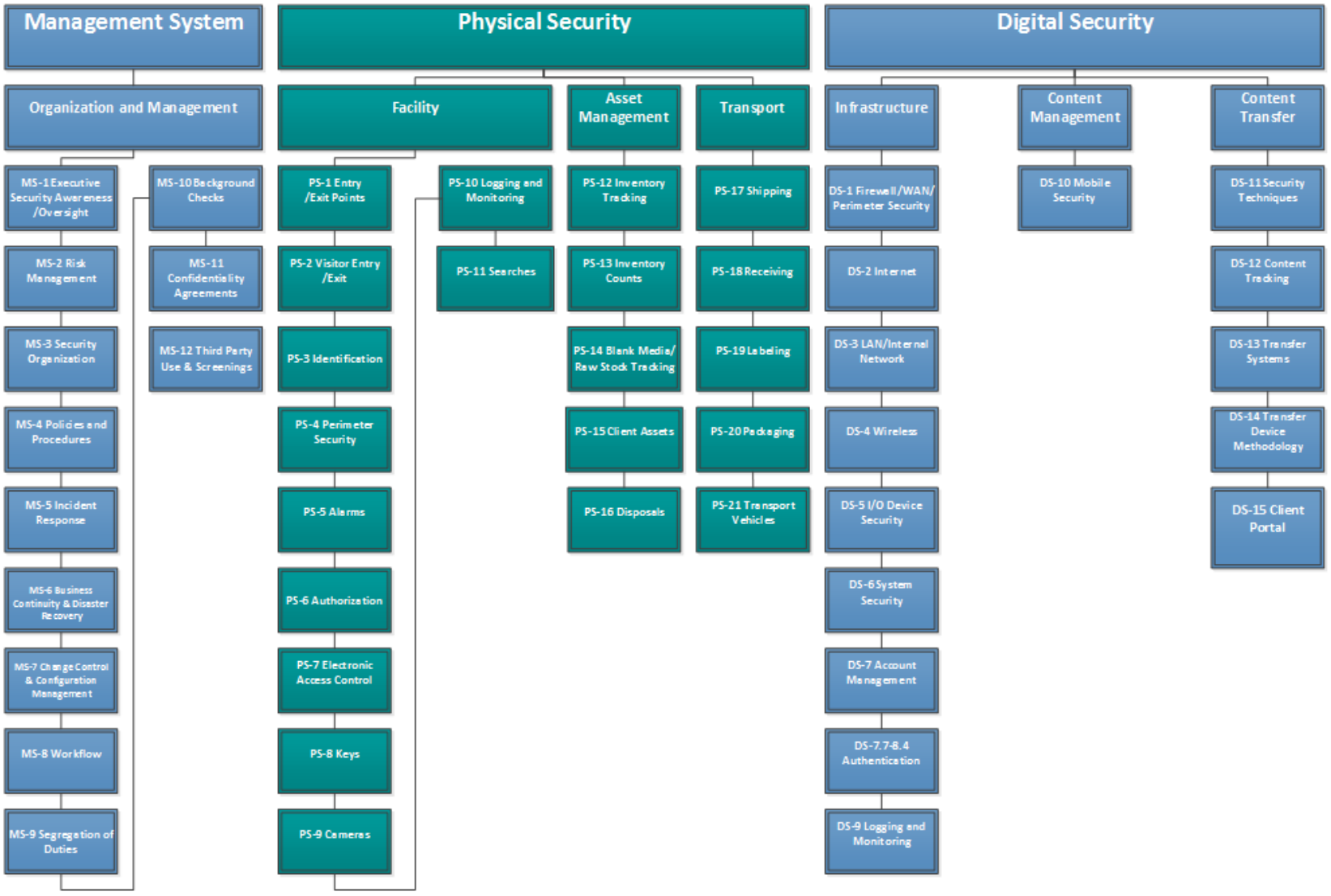
Security Controls

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.

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 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, CSA, ISACA and SANS) and industry best practices.



IV. BEST PRACTICES FORMAT

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

MANAGEMENT SYSTEM	PHYSICAL SECURITY			DIGITAL SECURITY		
ORGANIZATION AND MANAGEMENT	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 MPA Content Security Model.

No.	Security Topic	Best Practice	Implementation Guidance
PS-8.0	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-8.1		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.

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

V. BEST PRACTICE COMMON GUIDELINES

No.	Security Topic	Best Practice	Implementation Guidance
MS-1.0	Executive Security Awareness/ Oversight	Establish an information security management system that implements a control framework for information security which is approved by the business owner(s) / senior management.	• Reference established information and content security frameworks e.g. MPA Best Practices, ISO27001's, NIST 800-53, SANS, CoBIT, etc. • Establish an independent team for information security. Persons responsible for information security should not be working on content.
MS-1.1	Executive Security Awareness/ Oversight	Review content / information security management policies and processes at least annually. Policies must be approved by senior management.	Consider adjustments to policies and procedures from the following changes: • Organization's business, services offered, etc. • Technology infrastructure • Client requirements • Regulations or laws • Risk landscape
MS-1.2	Executive Security Awareness/ Oversight	Train and engage executive management/owner(s) on the business' responsibilities to protect content at least annually.	• Trainings and attendees should be documented in training logs
MS-1.3	Executive Security Awareness/ Oversight	Create an information security management group to establish and review information security management policies.	• Members of the information security management group should also attend security awareness training (see MS-1.2)
MS-2.0	Risk Management	Develop a formal, documented 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 and modify as necessary** • Incorporate a systematic approach that uses likelihood of risk occurrence, impact to business objectives/content protection and asset classification for assigning priority • Refer to MS-8.0 for best practices regarding documented **workflows**

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

No.	Security Topic	Best Practice	Implementation Guidance
MS-2.1	Risk Management	Conduct an internal security risk assessment annually and upon key workflow changes—based on, at a minimum, the MPA Best Practice Common Guidelines and the applicable Supplemental Guidelines—and document and act upon identified risks.	• Conduct meetings with management and key stakeholders at least quarterly to identify and document content theft and leakage risks • Conduct external and internal network vulnerability scans and external penetration testing, per DS-1.8 and DS-1.9 • Identify key risks that reflect where the facility believes content losses may occur • Implement and document controls to mitigate or reduce identified risks or where risks are being accepted with rationale (e.g. budget constraints, resource constraints etc.) • Monitor and assess the effectiveness of remediation efforts and implemented controls at least quarterly • Document and budget for security initiatives, upgrades, and maintenance • Indicate rationale for initiative/project prioritization (risk-based, cost-based, schedule based, etc.)
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

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

No.	Security Topic	Best Practice	Implementation Guidance
MS-4.0	Policies and Procedures	Establish policies and procedures regarding asset and content security; policies should address the following topics, at a minimum: • Acceptable use (e.g., social media, Internet, phone, personal devices, mobile devices, etc.) • Asset and content classification and handling policies • Business continuity (backup, retention and restoration) • Content transfer processes and systems • Change control and configuration management policy • Confidentiality policy • Digital recording devices (e.g., smart phones, digital cameras, camcorders) • Exception policy (e.g., process to document policy deviations) • Incident response policy • Mobile device policy • Network, internet and wireless policies • Password controls (e.g., password minimum length, screensavers) • Security policy • Visitor policy • Disciplinary/Sanction policy • Internal anonymous method to report piracy or mishandling of content (e.g., telephone hotline or email address)	• Consider facility/business-specific workflows in development of policies and procedures. • Require executive management to sign off on all policies and procedures before they are published and released • Communicate disciplinary measures in new hire orientation training • Please see Appendix D for a list of policies and procedures to consider

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

No.	Security Topic	Best Practice	Implementation Guidance
MS-4.0.1	Policies and Procedures	Establish dedicated policies governing the use of social media by company personnel.	• Social media policies should state that the following not be shared on any social media platform (e.g. Facebook, Twitter, IMDB, YouTube), forum, blog post, or website: Personal experiences, opinions and information related to pre-release content and related project activities References to clients without the express written consent from the client Posting, referencing or sharing of pre-release security or working titles • Use separate dedicated email accounts for marketing purposes when accessing social media platforms (e.g. Facebook, Twitter, IMDB, YouTube), forum, blog post, or website.
MS-4.0.2	Policies and Procedures	Establish policies governing the using of mobile computing devices.	• Address the following in mobile computing device policies: ○ BYOD if allowed: define the rights of the company and the rights of the owner, allowable devices / models ○ Acceptable use: corporate and personal ○ Restrictions on areas of the facility where mobile computing devices with recording capabilities are not allowed ○ Procedures for lost or stolen devices ○ Security measures (see Section DS-10)
MS-4.1	Policies and Procedures	Review and update security policies and procedures at least annually.	• Log/track versions & revisions • 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

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

No.	Security Topic	Best Practice	Implementation Guidance
MS-4.2	Policies and Procedures	Communicate and require sign-off from all **company personnel** (e.g., employees, temporary workers, interns) and **third party workers** (e.g., contractors, freelancers, temp agencies) for all current policies, procedures, and/or client requirements.	• Provide 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, procedures and client requirements • Management must retain sign-off of current policies, procedures, and client requirements for all **company personnel** and **third party workers**
MS-4.3	Policies and Procedures	Develop and regularly update an awareness program about security policies and procedures and train **company personnel** and **third party workers** upon hire and annually thereafter on those security policies and procedures, addressing the following areas at a minimum: • IT security policies and procedures • Content/asset security and handling in general and client-specific requirements • Social media policies • Social engineering prevention • Security incident reporting and escalation • Disciplinary policy • Encryption and key management for all individuals who handle encrypted content • Asset disposal and destruction processes	• Communicate security awareness messages during management/staff meetings • Implement procedures to track which **company personnel** have completed their annual security training (e.g., database repository, attendee logs, certificates of completion) • 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 • Distribute security awareness materials such as posters, emails, and periodic newsletters to encourage security awareness • Develop tailored messages and training based on job responsibilities and interaction with sensitive content (e.g., IT personnel, production) to mitigate piracy issues • Conduct social engineering education, training, and testing (see NIST SP 800-115 and SANS Methods for Understanding and Reducing Social Engineering Attacks) • Consider recording training sessions and making recordings available for reference

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

No.	Security Topic	Best Practice	Implementation Guidance
MS-5.0	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: Definition of incident Notification of security team Escalation to management Analysis of impact and priority Containment of impact Eradication and recovery Key contact information, including client studio contact information Notification of affected business partners and clients Notification of law enforcement Report of details of incident • Reference NIST SP800-61 Revision 2 on Computer Security Incident Handling
MS-5.1	Incident Response	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

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

No.	Security Topic	Best Practice	Implementation Guidance
MS-5.2	Incident Response	Establish a security incident reporting process for individuals to report detected incidents to the security **incident response** team.	• Consider implementing a group email address for reporting incidents that would inform all members of the incident response team • Communicate and document incidents promptly 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
MS-5.2.1	Incident Response	Anonymous reporting should be made available to organizations with 50 or more employees and third party personnel for reporting of content protection and piracy concerns. The anonymous reporting tool consisting of an internal, anonymous telephone number, email address, and / or website should be published and also provided during security awareness training.	
MS-5.3	Incident Response	*(Removed and combined with MS-5.2)*	

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

No.	Security Topic	Best Practice	Implementation Guidance
MS-6.0	Business Continuity & Disaster Recovery	Establish a formal plan that describes actions to be taken to ensure business continuity.	Consider including the following sections in the **business continuity** plan: • Threats to critical assets and content, including loss of power and telecommunications, systems failure, natural disasters etc. • Detailed information system, content and metadata backup procedures and information system documentation, including configuration of critical WAN and LAN / Internal Network devices • Encryption of backups (**AES-256**) • Backup power supply to support at least 15 minutes for the surveillance camera system, alarm and critical information systems, including software to perform a safe shutdown of critical systems • Consider use of an off-site backup location • Notification of security team • Escalation to management • Analysis of impact and priority • Containment of impact • Priorities for recovery and detailed recovery procedures, including manual workarounds and configuration details of restored systems • Key contact information • Notification of affected business partners and clients • Testing of business continuity and disaster recovery processes at least annually
MS-6.1	Business Continuity & Disaster Recovery	Identify the business continuity team who will be responsible for detecting, analyzing and remediating continuity incidents.	• Include defined roles and responsibilities • Provide training so that members of the business continuity team understand their roles and responsibilities

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

No.	Security Topic	Best Practice	Implementation Guidance

MS-6.2	Business Continuity & Disaster Recovery	Establish a data backup policy that addresses the following:
		
		• Systems and data
		• Retention and protection requirements
		• Backup frequency
		• Encryption
		• Recovery time objectives (RTO)
		• Recovery point objectives (RPO)
		• Restoration testing
		• Secure offsite storage
			• Align backup policy with the business continuity plan
			• Implement physical and environmental security controls (per MPA guidelines) for offsite storage to prevent unauthorized access or stolen / lost content
			• Encrypt backups using AES with at least 256 bit key before storing content offsite in remote locations or on the cloud
			• Notify clients if the cloud backups will be used
			• Frequency of backups and recovery testing must be based on RTO and RPO that meets client requirements. The following is recommended:
			  • Daily incremental and weekly backups
			  • RTO of 48 hours or less for client content
			  • Quarterly data restoration testing
			• Review process should be in place to ensure that only authorized administrators are able to access backup location

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

No.	Security Topic	Best Practice	Implementation Guidance

MS-7.0	Change Control & Configuration Management	Establish policies and procedures to ensure new data, applications, network, and systems components have been pre-approved by business leadership.	• Include documentation that describes installation, configuration and use of devices, services and features, and update documentation as needed
			• Document known issues and procedures for dealing with them
			• Include procedures for reporting bugs and security vulnerabilities
			• Restrict and monitor the installation of hardware or software
			• Manage risks associated with changes to data, applications, network infrastructure and systems
			  ○ Review security controls and integrity procedures to ensure they will not be compromised by changes
			  ○ Ensure that appropriate backup or roll-back procedures are documented and tested
			  ○ Identify all affected computer software, data files, database entities, and infrastructure
			  ○ Minimize business disruption when implementing change
			• Document and retain all change requests, testing results and management approvals

MS-8.0	Workflow	Document **workflows** tracking content and authorization checkpoints. Include the following processes for both physical and digital content: • Delivery (receipt/return) • Ingest • Movement • Storage • Removal/destruction	• Use swim lane diagrams to document **workflows** • Include asset processing and handling information where applicable • Evaluate each touch-point for risks to content • Implement controls around authorization checkpoints • Identify related application controls • Update the **workflow** when there are changes to the process, and review the **workflow** process at least annually to identify changes. • Follow the content **workflow** and implemented controls for each process in order to determine areas of vulnerability
MS-8.1	Workflow	*(Removed and combined with MS-8.0)*	

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

No.	Security Topic	Best Practice	Implementation Guidance
MS-9.0	Segregation of Duties	Segregate duties within the content **workflow**. Implement and document compensating controls where segregation is not practical.	• 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**) • 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
MS-10.0	Background Checks	Perform background screening checks on all **company personnel**, **third party workers,** and their relevant subcontractors.	• 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

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

No.	Security Topic	Best Practice	Implementation Guidance
MS-11.0	Confidentiality Agreements	Require all **company personnel** to sign a confidentiality agreement (e.g., non-disclosure) upon hire and review 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 • Ensure all relevant information on equipment used by **company personnel** to handle business-related sensitive content is transferred to the organization and securely removed from the equipment • Management must retain signed confidentiality agreements for all **company personnel**
MS-11.1	Confidentiality Agreements	Require all **company personnel** to return all content and client information in their possession upon termination of their employment or contract.	• Utilize an off boarding process for terminated employees to ensure the following: ○ all content and client information is returned ○ company equipment and property is returned ○ keys, access cards, badges are returned ○ reasons for termination are documented ○ user accounts / access rights on all systems are removed or disabled ○ Documenting and storing a history of terminated personnel for five years at a minimum ○ Formally reminding departing personnel of their ongoing confidentiality and non-disclosure responsibilities
MS-12.0	Third Party Use and Screening	Require all **third party workers** (e.g., freelancers) 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 • Explain the importance of confidentiality / NDA in non-legal terms, as necessary • Ensure all relevant information on equipment used by **third party workers** to handle business-related sensitive content is transferred to the organization and securely removed from the equipment • Management must retain signed confidentiality agreements for all **third party workers** • Include requirements for handling and protecting content

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

No.	Security Topic	Best Practice	Implementation Guidance
MS-12.1	Third Party Use and Screening	Require all **third party workers** to return all content and client information in their possession upon termination of their contract.	
MS-12.2	Third Party Use and Screening	Include security requirements in third party contracts.	• Service Level Agreements (SLAs) and contracts with the third party vendors should the following provisions: Require **third party workers** to comply with the security requirements per MPA Best Practices A right to audit clause for activities that involve sensitive content Notification to clients upon suspected or actual security breaches Content ownership, return, and destruction Termination clause • Implement a process to monitor for compliance with security requirements • Require annual update of information when contracts are renewed
MS-12.3	Third Party Use and Screening	Implement a process to reclaim **content** when terminating relationships with third party service providers.	• Ensure all **content** on third party equipment is transferred to the organization and securely erased from the equipment
MS-12.4	Third Party Use and Screening	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 annual update of information when contracts are renewed
MS-12.5	Third Party Use and Screening	Restrict third party access to content / production areas unless required for their job function.	• Ensure that **third party workers** who do not handle content (e.g., cleaning crews, HVAC maintenance, etc.) are not given any access to areas housing or exhibiting content • Escort **third party workers** who do not handle content when access to restricted areas (e.g., **vault**) is required

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

No.	Security Topic	Best Practice	Implementation Guidance
MS-12.5.1	Third Party Use and Screening	Control access of third party IT service providers to the computing environment.	• Third-party VPN remote access should only be used in cases where no other solution is available. Client approval is required in writing. • All third-party VPN remote access should have a finite end date and be reviewed for activity every three months at a minimum • Third-party VPN remote access should not provide access to network infrastructure that includes networks or systems used to store, transfer, or manipulate content • All third-party access sessions should be monitored by an employee and logged • Log and monitor IT service providers access to systems, networks, and infrastructure • Third-party systems used for remote access should be subjected to an inspection, by an employee, on a periodic and ongoing basis • IT service provider remote access must utilize multi-factor authentication • Disable IT service provider remote access when not needed • Change remote access passwords for every session • Follow change control processes for elevating user access rights • Consider real-time notification when IT service providers access systems

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

No.	Security Topic	Best Practice	Implementation Guidance

MS-12.6	Third Party Use and Screening	Notify clients if third parties are used to handle or store content, or work is offloaded to another company. Perform due diligence of third parties.
		
		Third parties also include providers of IT services. Obtain client approval for use of third parties who handle, store, or have access to content.
			• Work offloaded to another company must be reported to the content owners and requires written client sign-off / approval
			• Production servers and systems hosted on third-party networks must be vetted by content owners prior to deployment.
			• Cloud-Hosted systems and servers are strictly prohibited without advanced written consent of content owners.
			• Workflows using cloud hosted servers should be approved by content owners.
			• Perform due diligence and ongoing monitoring of third parties to verify the following:
			  ○ Security controls meet MPA Best Practices
			  ○ Adequate level of insurance coverage (refer to MS-12.4)
			  ○ Viable financial state
			• Request that third parties obtain an independent security assessment for submission to the member studios

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

No.	Security Topic	Best Practice	Implementation Guidance
PS-1.0	Entry/Exit Points	Secure all entry/exit points of the facility at all times, including loading dock doors and windows.	• 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	Entry/Exit Points	Control access to areas where content is handled by segregating the content area from other facility areas (e.g., administrative offices, waiting rooms, loading docks, courier pickup and drop-off areas, replication and mastering).	• Allow access to content / production areas on a need-to-know basis • 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) • Enforce a segregation of duties model which restricts any single person from having access to both the replication and mastering rooms
PS-1.2	Entry/Exit Points	Control access where there are collocated businesses in a facility, which includes but is not limited to the following: • Segregating work areas • Implementing access-controlled entrances and exits that can be segmented per business unit • Logging and monitoring of all entrances and exits within facility • All tenants within the facility must be reported to client prior to engagement	
PS-2.0	Visitor Entry/Exit	Maintain a detailed visitors' log and include the following: • Name • Company • Time in/time out • Reason for visit • Person/people visited • Signature of visitor • Badge number assigned	• Verify the identity of all visitors by requiring them to present valid photo identification (e.g., driver's license or government-issued ID) • Consider concealing the names of previous visitors • The facility should retain visitor logs for twelve months at a minimum.

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

No.	Security Topic	Best Practice	Implementation Guidance
PS-2.1	Visitor Entry/Exit	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 • Facilities that have less than 25 employees are not required to have visitor badges
PS-2.2	Visitor Entry/Exit	Do not provide visitors with key card access to content / production areas.	
PS-2.3	Visitor Entry/Exit	Require visitors to be escorted by authorized employees while on-site, or in content / production areas.	
PS-2.3.1	Visitor Entry/Exit	Visitors should be required to sign a nondisclosure agreement (NDA) and sign a visitor log prior to entering a facility.	
PS-3.0	Identification	Provide **company personnel** and long-term **third party workers** (e.g., janitorial) with a photo **identification badge** that is required to be visible at all times.	• Issue photo **identification badge** 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 **identification badge** upon termination • Consider omitting location, company name, logo and other specific information on the photo **identification badge** • Consider using the **photo identification badge** as the access key card where possible • Require employees to immediately report lost or stolen **photo identification badges** • Provide a 24/7 telephone number or website to report lost or stolen **photo identification badges** • Train and encourage employees to challenge persons without visible identification

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

No.	Security Topic	Best Practice	Implementation Guidance
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 • Securing and enclosing, as necessary, common external areas such as smoking areas and open balconies • Installing lighting with full coverage outside the facility to decrease risk of theft or security violations • 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 • Glass break sensors as necessary • Using alarms around the perimeter, as necessary
PS-4.1	Perimeter Security	Place security guards at perimeter entrances and non-emergency entry/exit points.	**Note:** Not all sites require security guards. This should be determined based on risk, per MS-2.1
PS-4.2	Perimeter Security	Implement a daily security patrol process with a randomized schedule and document the patrol results in a log.	Consider the following if applicable: • Require security guards to patrol both interior and exterior areas • Include a review of emergency exits, including verification of seals • Use a guard tour patrol system to track patrolling (e.g., checkpoint) and verify locks
PS-4.3	Perimeter Security	Lock perimeter gates at all times.	Consider the following if applicable: • Implement an electronic arm, that is manned by security personnel, to control vehicle access into the facility • Distribute parking permits to company personnel and third party workers who have completed proper paperwork • Require visitor vehicles to present identification and ensure that all visitors have been pre-authorized to enter the premises

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

No.	Security Topic	Best Practice	Implementation Guidance
PS-5.0	Alarms	Install a centralized, audible alarm system that covers all entry/exit points (including emergency exits), windows, loading docks, fire escapes, and restricted areas (e.g., **vault**, server/machine room, etc.).	• Place alarms at every entrance to alert security personnel upon unauthorized entry to the facility • Enable the alarm when facility is unsupervised
PS-5.1	Alarms	Install and effectively position motion detectors in restricted areas (e.g., **vault**, server/machine room) and configure them to alert the appropriate security and other personnel (e.g. project managers, producer, head of editorial, incident response team, etc.).	• 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-5.2	Alarms	Install door prop alarms in restricted areas (e.g. vault, server, machine rooms) 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-5.3	Alarms	Configure alarms to provide escalation notifications directly to the personnel in charge of security and other personnel (e.g., project managers, producer, head of editorial, incident response team, etc.).	• 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-5.4	Alarms	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 individuals responsible for arming or disarming the alarm • Update assigned alarm codes at an interval approved by management in order to reduce risk involved with sharing and losing codes • Issue alarm codes to personnel on a least privilege basis • Security personnel, contractors, vendors, cleaning crews, and freelance staff should not have administrator rights to the alarm system • Alarm notifications should be sent to appropriate company personnel according to an escalation tree.

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

No.	Security Topic	Best Practice	Implementation Guidance
PS-5.5	Alarms	Review the list of users who can arm and disarm alarm systems quarterly, or upon change of personnel.	• Remove users who have left the company or have changed job roles • Deactivate the alarm codes that were assigned to removed users
PS-5.6	Alarms	Test the alarm system quarterly.	• 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-5.7	Alarms	Implement fire safety measures so that in the event of a power outage, fire doors fail open, and all others fail shut to prevent unauthorized access.	
PS-6.0	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-6.1	Authorization	Restrict access to production systems to authorized personnel only.	
PS-6.2	Authorization	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

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

No.	Security Topic	Best Practice	Implementation Guidance
PS-7.0	Electronic Access Control	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 electronic access device number to company personnel • See Logging and Monitoring PS-10.0 • Review the times when electronic access is not required for common areas (e.g., public elevators)
PS-7.1	Electronic Access Control	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-7.2	Electronic Access Control	Store card stock and **electronic access devices** (e.g., keycards, key fobs) in a locked cabinet and ensure **electronic access devices** remain disabled prior to being assigned to personnel. Store unassigned electronic access devices (e.g., keycards, key fobs) in a locked cabinet and ensure these remain disabled prior to being assigned to personnel.	• Limit access to the locked cabinet to the **keycard** / **electronic access device** system administration team • Require sign-out for inventory removal
PS-7.3	Electronic Access Control	Disable lost **electronic access** devices (e.g., keycards, key fobs) in the system before issuing a new **electronic access device**.	• Educate **company personnel** and **third party workers** to report lost **electronic access devices** immediately to prevent unauthorized access into the facility • Require identification before issuing replacement **electronic access devices**
PS-7.4	Electronic Access Control	Issue third party access **electronic access devices** with a set expiration date (e.g. 90 days) based on an approved timeframe.	• Ensure that third **party electronic access devices** are easily distinguishable from **company personnel** electronic access devices • Ensure that expiration date is easily identifiable on the **electronic access devices** • Assign third **party** electronic access devices on a need-to-know basis

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

No.	Security Topic	Best Practice	Implementation Guidance
PS-8.0	Keys	Limit the distribution of **master keys** and / or keys to restricted areas 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-8.1	Keys	Implement a check-in/check-out process to track and monitor the distribution of **master keys** and / or keys to restricted areas.	• 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-8.2	Keys	Use keys that can only be copied by a specific locksmith for exterior entry/exit points.	• 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-8.3	Keys	Inventory **master keys** and keys to restricted areas, including facility entry/exit points, quarterly.	• Identify, investigate, and address any missing keys (lost/stolen) • 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-8.4	Keys	Obtain all keys from terminated employees/third-parties or those who no longer need the access.	
PS-8.5	Keys	Implement electronic access control or rekey entire facility when master or sub-master keys are lost or missing.	

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

No.	Security Topic	Best Practice	Implementation Guidance
PS-9.0	Cameras	Install a surveillance camera system (analog CCTV or IP cameras) that records all facility entry/exit points and restricted areas (e.g. server/machine room, etc.).	• Camera cables and wiring should be discretely hidden from view and not within reasonable reach • Facility should not assume that cameras provided by the building are adequate • Place cameras at every entrance / exit to the facility • Ensure the cameras cover storage areas and **vaults** • Cameras in server / machine rooms should cover both the front and back of the racks • Use rack mounted cameras to provide coverage of the ports of computing equipment where content resides; this applies to instances where other cameras have an obscured view of the ports (e.g., equipment housed at colocation data centers.)
PS-9.1	Cameras	Review camera positioning and recordings to ensure adequate coverage, function, image quality, lighting conditions, and frame rate of surveillance footage at least daily.	• Position cameras to ensure an unobstructed view of all entry/exit points and other sensitive areas • Position and orient cameras to capture facial features that might be partially obstructed by hats, hoods, or other worn headgear • Accommodate for cameras in dark areas (e.g., low-light or infrared cameras, motion-detecting lights) • Implement sufficient image quality and lighting to ensure that faces are distinguishable. Record with sufficient resolution to identify facial features • Set frame rate to ensure that activity is adequately recorded. Record at a minimum rate of 7 frames per second • Position and orient cameras to avoid capturing content on display

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

No.	Security Topic	Best Practice	Implementation Guidance
PS-9.2	Cameras	Restrict physical and/or logical access to the surveillance camera **console** and to camera equipment (e.g., DVRs, NVRs) to personnel responsible for administering/monitoring the system	• Place camera 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 adheres to the following: 1. camera system is restricted to authorized personnel 2. Strong account management controls are in place (e.g., password complexity, individual user login, logging and monitoring) 3. Consider restricting administrative access to the local LAN only 4. Consider enabling Multi-Factor Authentication (MFA) for access to the camera system 5. Camera footage should be stored locally. Client approval must be obtained if cloud storage of footage is being considered 6. The camera system should be restricted to its own dedicated LAN and connections from this LAN to the networks that handle content should not be allowed
PS-9.3	Cameras	Ensure that camera footage includes an accurate date and time-stamp and retain camera surveillance footage and electronic access logs for at least 90 days, or the maximum time allowed by law, in a secure location.	• 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 • Review date and time stamp for accuracy at least weekly • 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 • Consider retaining camera surveillance footage until the first production release date

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

No.	Security Topic	Best Practice	Implementation Guidance
PS-9.4	Cameras	Designate an employee or group of employees to monitor surveillance footage during operating hours and immediately investigate detected security incidents.	• Incorporate the incident response process for handling security incidents • Consider adding a surveillance monitor at the reception desk or in the IT office
PS-10.0	Logging and Monitoring	Log and review electronic access to restricted areas for suspicious events, at least weekly.	• 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 • Retain logs for one year, at a minimum • Log and review the following events: Repeated failed access attempts Unusual time-of-day access Successive door access across multiple zones
PS-10.1	Logging and Monitoring	Log and review electronic access, at least daily, for the following areas: • Masters/stampers vault • Pre-mastering • Server/machine room • Scrap room • High-security cages	• Identify and document events that are considered unusual • 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.
PS-10.2	Logging and Monitoring	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-10.3	Logging and Monitoring	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 / electronic access device** incidents • Review all recent **keycard / electronic access device** incidents periodically and perform root-cause analysis to identify vulnerabilities and appropriate fixes

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

No.	Security Topic	Best Practice	Implementation Guidance
PS-11.0	Searches	Establish a policy, as permitted by local laws, which allows security to randomly search persons, bags, packages, and personal items for client content.	• Communicate policies regarding search to all **company personnel** and **third party workers** • Consider conducting searches periodically of **company personnel** and **third party workers** to validate policy **Note**: Not all sites require a search policy. This should be determined based on risk per MS-2.1 and facility type.
PS-11.1	Searches	Implement an exit search process that is applicable to all facility personnel and visitors, including: • Removal of all outer coats, hats, and belts for inspection • Removal of all pocket contents • Performance of a self-pat-down with the supervision of security • Thorough inspection of all bags • Inspection of laptops' CD/DVD tray • Scanning of individuals with a handheld metal detector used within three inches of the individual searched	• Instruct security guards to look for items that are restricted from being brought onsite (e.g., cameras) or film materials which are not allowed to be brought offsite without proper authorization • Communicate policies regarding exit search to all company personnel and third party workers • Stagger shift changes to prevent long lines and extended wait times • This control is only applicable for facilities that perform CD/DVD or other physical device replication and where laws allow implementation
PS-11.2	Searches	Prohibit personnel from entering/exiting the facility with digital recording devices (e.g., **USB** thumb drives, digital cameras, cell phones) and include the search of these devices as part of the exit search procedure.	• Confiscate any digital recording devices that are detected and store them in secured lockers • Document any incidents of attempted content theft • Take the necessary disciplinary action for individuals attempting content theft • Implement and enforce a policy to prohibit mobile/cellular devices with digital recording capabilities • Allow cell phones with digital recording capabilities if tamper-evident stickers are used • If an exception has been documented and approved in writing by the client that permits use of digital devices in restricted areas, use of those devices when content is open and viewable is still prohibited
PS-11.3	Searches	Enforce the use of transparent plastic bags and food containers for any food brought into production areas.	• Consider designating an area for eating food outside of the production area

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

No.	Security Topic	Best Practice	Implementation Guidance
PS-11.4	Searches	Implement a dress code policy that prohibits the use of oversized clothing (e.g., baggy pants, oversized hooded sweatshirts).	
PS-11.5	Searches	Use numbered tamper-evident stickers/holograms to identify authorized devices that can be taken in and out of the facility.	
PS-11.6	Searches	Implement a process to test the exit search procedure.	• Perform periodic audits of the search process to ensure that security guards are thorough with their searches • Identify ways to improve the exit search process • Document all audits of and improvements to the search process
PS-11.7	Searches	Perform a random vehicle search process when exiting the facility parking lot.	
PS-11.8	Searches	Segregate replication lines that process highly sensitive content and perform searches upon exiting segregated areas.	
PS-11.9	Searches	Implement additional controls to monitor security guards activity.	• Review the exit search process for security guards upon exit • Segregate security guard responsibilities for overseeing plant/production areas from exit points (e.g., search process)

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

No.	Security Topic	Best Practice	Implementation Guidance
PS-12.0	Inventory Tracking	Implement a content asset management system to provide detailed tracking of physical assets (i.e., received from client created at the facility).	• 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 • Consider the use of an automated alert to provide notifications of assets that have not been returned by end of the business day, or the authorized period of time • 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-12.1	Inventory Tracking	Barcode or assign unique tracking identifier(s) to 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 barcoded and return assets to the **vault** immediately when no longer needed
PS-12.1.1	Inventory Tracking	Develop a data classification scheme to categorize physical assets of differing security requirements. *(Reordered and renumbered, previously PS-12.1.2)*	• Define security levels of content according to risk • Ensure data classifications are consistent with client requirements • Data classification schemes are particularly important in facilities that work on different types of content, e.g. catalog, TV, and theatrical in same environment
PS-12.2	Inventory Tracking	Retain asset movement transaction logs for at least one year.	• 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

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

No.	Security Topic	Best Practice	Implementation Guidance
PS-12.3	Inventory Tracking	Review logs from content **asset management** system at least weekly 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-12.4	Inventory Tracking	Use studio film title aliases on physical assets and in asset tracking systems.	• Consider removing the studio name on physical assets, when appropriate
PS-12.5	Inventory Tracking	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-12.5.1	Inventory Tracking	A documented process for checking out content should be established.	Guidelines should include, but are not limited to: • Ensuring that checkout durations not exceed 24 hours or the duration of the custodian's shift unless explicitly approved in writing by management • Performing daily inventory checks to track content and investigate individuals who have not returned content in a timely manner • Using automatic system notifications to alert team members when content has not been returned within the expected timeframe
PS-12.6	Inventory Tracking	Lock up and log assets that are delayed or returned if shipments could not be delivered on time.	• Establish a procedure for storing assets in an access-controlled area • Maintain documentation that logs the on-site storage of assets, including the date and reason for storage
PS-13.0	Inventory Counts	Perform a quarterly inventory count of each client's asset(s), reconcile against **asset management** records, and immediately communicate variances to clients.	
PS-13.1	Inventory Counts	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

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

No.	Security Topic	Best Practice	Implementation Guidance
PS-14.0	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-14.1	Blank Media/ Raw Stock Tracking	Establish a process to track consumption of raw materials (e.g., polycarbonate) monthly.	• Reconcile existing raw stock with work orders to identify variances in inventory • Establish a variance threshold that triggers the **incident response** process when exceeded • Consider the execution of physical counts of raw stock as part of the monthly tracking process
PS-14.2	Blank Media/ Raw Stock Tracking	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
PS-15.0	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-15.1	Client Assets	Store client assets in a restricted and secure area (e.g., **vault**, safe, or other secure storage location).	• Implement an additional safe or high-security cage within the **vault** for highly sensitive titles • Sensitive content should also be stored in a secure segregated area (e.g., safe, cage or other isolated area) and segregated from other content • A safe weighing less than 300 lbs. should be secured to an immovable surface (e.g., floor, wall). Note: Bolting the safe may make its' contents vulnerable to fire damage. This is not recommended for storing backups
PS-15.2	Client Assets	Consider requiring two company personnel with separate access cards or keys / pins to unlock highly sensitive areas (e.g., safe, high-security cage) after-hours.	

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

No.	Security Topic	Best Practice	Implementation Guidance
PS-15.3	Client Assets	Use a locked fireproof safe to store undelivered packages that are kept at the facility overnight.	
PS-15.4	Client Assets	Implement a dedicated, secure area (e.g., security cage, secure room) for the storage of undelivered screeners that is locked, access-controlled, and monitored with surveillance cameras and/or security guards.	• Limit access to personnel who require access for their job role • Ensure that the screener storage area is completely enclosed, locked and monitored at all times • Implement a process to review surveillance footage on a regular basis
PS-16.0	Disposals	Require that rejected, damaged, and obsolete stock (DVDs, tapes, and other storage media) containing client assets are erased, degaussed, shredded, or physically destroyed before disposal.	• Implement processes to inventory and reconcile stock, and then securely recycle or destroy rejected, damaged, and obsolete stock • Irreparably damage media before placing into scrap bin • Consider referencing U.S. Department of Defense 5220.22-M for digital shredding and wiping standards
PS-16.0.1	Disposals	Finished elements (e.g., check discs, test prints, mock-ups, ADR scripts) should be destroyed immediately after use, unless otherwise specified by content owners. Require paper materials containing client assets (scripts, artwork, storyboards, etc.) be physically destroyed before disposal.	• Shredders must cut paper in a cross-hatch pattern • Shred bins must be locked with openings small enough that a hand cannot fit inside • Restrict keys to shred bins on a least privilege basis • Purge Copier hard drives on at least a weekly basis
PS-16.1	Disposals	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-16.2	Disposals	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

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

No.	Security Topic	Best Practice	Implementation Guidance
PS-16.3	Disposals	Destruction must be performed on site. On site destruction must be supervised and signed off by two company personnel. If a third party destruction company is engaged, destruction must be supervised and signed off by two company personnel and certificates of destruction must be retained.	• 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-16.4	Disposals	Use automation to transfer rejected discs from replication machines directly into scrap bins (no machine operator handling).	• Use segregation of duties (e.g., personnel who create the check disc are separate from personnel who destroy the disc) where automated disposal is not an option • Maintain a signed log of the date and time when the disc was disposed
PS-17.0	Shipping	Require the facility to generate a valid work/shipping order to authorize client 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 • Create a form for documenting outbound assets that are transported via uncommon methods
PS-17.1	Shipping	Track and log client 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 of 1 year

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

No.	Security Topic	Best Practice	Implementation Guidance
PS-17.2	Shipping	Secure client assets that are waiting to be picked up.	• Lock all doors and windows to shipping and receiving areas when unattended • Assets must be locked up until handed off to the vendor/courier • Camera surveillance should be used to monitor content that is being staged prior to shipping. If appropriate, it should also be used to capture the transfer of a package from the facility to the courier. • Drives, reels, DVDs to be shipped should be brought to the public loading area only after the truck arrives.
PS-17.3	Shipping	Validate client 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 • Report back any discrepancies or damage to shipped goods immediately
PS-17.4	Shipping	Prohibit couriers and delivery personnel from entering content / production areas of the facility.	• Escort delivery personnel if access to content / production areas is necessary
PS-17.5	Shipping	Document and retain a separate log for truck driver information.	• Maintain a log of all truck drivers and include the following information: Name License tags for the tractor and trailer Affiliated company Time and date of pick up Content handled
PS-17.5.1	Shipping	Facilities should implement and maintain a record of all delivery personnel entering and exiting the building.	
PS-17.6	Shipping	Observe and monitor the on-site packing and sealing of trailers prior to shipping.	• Require security personnel to be present at all times while trailers are loaded and sealed

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

No.	Security Topic	Best Practice	Implementation Guidance
PS-17.7	Shipping	Record, monitor and review travel times, routes, and delivery times for shipments between facilities.	• Establish a baseline for delivery times between common shipping points and monitor actual times for variance • Investigate, report, and escalate major variances to appropriate personnel • Designate approved rest stops • Consider implementing a real-time GPS tracking system to monitor and alert on unexpected delays
PS-17.8	Shipping	Prohibit the transfer of film elements outside of the shipping department unless approved by the client.	• Treat film elements like any other piece of physical media, using the same controls for shipping and receiving.
PS-17.9	Shipping	Ship prints for pre-theatrical screenings in segments (e.g., odd versus even reels).	
PS-18.0	Receiving	Inspect delivered client assets 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-18.1	Receiving	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-18.2	Receiving	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-18.3	Receiving	Implement a secure method for receiving overnight deliveries.	• Ensure that schedules for expected items are only available to people who need to see them
PS-19.0	Labeling	Prohibit the use of title information, including AKAs ("aliases"), on the outside of packages unless instructed otherwise by client.	

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

No.	Security Topic	Best Practice	Implementation Guidance
PS-20.0	Packaging	Ship all client assets in closed/sealed containers, and use locked containers depending on asset value, or if instructed by the client.	
PS-20.1	Packaging	Implement at least one of the following controls: • Tamper-evident tape • Tamper-evident packaging • Tamper-evident seals (e.g., in the form of holograms) • Secure containers (e.g., Pelican case with a combination lock)	• Establish and communicate a plan for how to handle goods that have been tampered with • Report all instances of tampering to the Incident Response Team (MS-5.0)
PS-20.2	Packaging	Apply shrink wrapping to all shipments, and inspect packaging before final shipment to ensure that it is adequately wrapped.	• Apply shrink wrapping to individual assets (e.g., skids, pallets) or per spindle if bulk shipments are performed
PS-21.0	Transport Vehicles	Lock automobiles and trucks at all times, and do not place packages in clear view.	• Do not leave packages unattended
PS-21.1	Transport Vehicles	Include the following security features in transportation vehicles (e.g., trailers): • Segregation from driver cabin • Ability to lock and seal cargo area doors • GPS for high-security shipments	• Use vehicles equipped with GPS tracking systems for delivery of sensitive content and high-value assets
PS-21.2	Transport Vehicles	Apply numbered seals on cargo doors for shipments of highly sensitive titles.	• Require security guards to apply, record, and monitor seals • Consider additional security measures for highly sensitive packages (e.g., locked/secured cargo area, locked pelican cases
PS-21.3	Transport Vehicles	Require security escorts to be used when delivering highly sensitive content to high-risk areas.	• Hire security personnel capable of protecting highly sensitive content from hijacking, mugging, and other scenarios that could result in content theft

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

No.	Security Topic	Best Practice	Implementation Guidance
PS-22.0	Environmental	Maintain optimal temperature and humidity set-points to facilitate optimal performance of equipment and to reduce the likelihood of catastrophic hardware failures for areas that house servers, storage devices, LAN equipment, network communications devices, and storage media.	• Recommended temperature and humidity settings: Temperature (Low End): 64.4 F (18 C) Temperature (High End): 80.6 (27 C) Moisture (Low End): 40% relative humidity and 41.9 F (5.5 C) dew point Moisture (High End): 60% relative humidity and 59 F (15 C) dew point

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

No.	Security Topic	Best Practice	Implementation Guidance
DS-1.0	Firewall / WAN / Perimeter Security	Separate external network(s)/WAN(s) from the internal network(s) by using inspection firewall(s) with Access Control Lists that prevent unauthorized access to any internal network and with the ability to keep up with upload and download traffic.	• 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 • Include detailed WAN documentation that accurately shows and describes the number of connections to and from all external facing devices • Firewall rules must be configured to generate logs for all traffic and for all configuration changes, and logs should be inspected on at least a monthly basis • Firewall should have a subscription to anti-virus and intrusion detection updates, and updates should occur at least once per week • Consider including the following in the firewall configuration: Anti-spoofing filters Block non-routable IP addresses Block internal addresses over external ports Block UDP and ICMP echo requests Block unused ports and services Block unauthorized DNS zone transfers Apply egress filtering, so outgoing traffic can only come from an internal address
DS-1.1	Firewall / WAN / Perimeter Security	Implement a process to review firewall Access Control Lists (**ACL**s) to confirm configuration settings are appropriate and required by the business every 6 months.	• Export **ACL**s from firewalls and/or routers • Review **ACLs** to confirm that network access is appropriate • Require management sign-off of review, as well as any firewall rule changes • Records of all externally accessible servers as well as each business case and system owner of each server should be maintained • Update **ACLs** accordingly

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

No.	Security Topic	Best Practice	Implementation Guidance
DS-1.2	Firewall / WAN / Perimeter Security	Deny all incoming and outgoing network requests by default. Enable only explicitly defined incoming requests by specific protocol and destination. Enable only explicitly defined outgoing requests by specific protocol and source.	• Block all unused ports and services • For externally accessible hosts, only allow incoming requests to needed ports on those hosts • Restrict all unencrypted communication protocols such as **Telnet** and **FTP** • Replace unencrypted protocols with encrypted versions
DS-1.3	Firewall / WAN / Perimeter Security	Place externally accessible servers (e.g., web servers) within the **DMZ**.	• Isolate servers in the **DMZ** to provide only one type of service per server (e.g., web server, etc.) • Implement **ACLs** to restrict access to the internal network from the **DMZ**
DS-1.4	Firewall / WAN / Perimeter Security	Implement a process to patch network infrastructure devices (e.g., firewalls, routers, switches, etc.), SAN/NAS (Storage Area Networks and Network Attached Storage), and servers.	• Implement a regular (e.g. monthly) process to identify, evaluate and test patches for network infrastructure devices, SAN/NAS and servers • Update network infrastructure devices, SAN/NAS, and servers to patch levels that address significant security vulnerabilities • Address critical patches within 48 hours • Consider the deployment of a centrally managed patch management system
DS-1.5	Firewall / WAN / Perimeter Security	Harden network infrastructure devices, SAN/NAS, and servers based on security configuration standards. Disable SNMP (Simple Network Management Protocol) if it is not in use or use only SNMPv3 or higher and select SNMP community strings that are strong passwords.	• Consider the following hardening options: Disable guest accounts and shares Install anti-virus / anti-malware Enable software firewalls Remove unnecessary software Uninstall/disable unneeded services Require all users to run as restricted users Use an **ACL** that restricts access to the device so that only authorized management systems may be used to connect using SNMP • Refer to the following security hardening standards for hardening network infrastructure devices: NIST SANS NSA

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

No.	Security Topic	Best Practice	Implementation Guidance
DS-1.6	Firewall / WAN / Perimeter Security	Do not allow direct management of the firewall from any external interfaces (i.e. Internet or WAN facing).	• Instead use two-factor authentication and a **VPN** connection with advanced encryption standard (**AES-256**) to carry out remote administration functions • Require individuals to provide two of the following for non-administrative remote access: Information that the individual knows (e.g., username, password) A unique physical item that the individual has (e.g., token, **keycard,** smartphone, certificate) A unique physical quality/biometrics that is unique to the individual (e.g., fingerprint, retina)
DS-1.7	Firewall / WAN / Perimeter Security	Store local backups of network infrastructure / SAN/NAS devices and servers on a server in a secure internal network.	• Configure network infrastructure devices to store backups of configuration files in a secure manner (e.g., encrypted) on the internal network • Ensure that only authorized administrators have access to the storage location and the encrypted backups • 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	Firewall / WAN / Perimeter Security	Perform on at least a monthly basis network vulnerability scans of all external IP ranges and hosts and remediate issues.	• Remediate critical issues that could allow unauthorized access to content within 48 hours. • Remediate non critical issues in a timely manner • Ensure that tools used for scanning/testing accommodate virtualization technologies, if being used • Consider having this performed by an independent third-party
DS-1.9	Firewall / WAN / Perimeter Security	Perform on at least an annual basis, penetration testing of all external IP ranges and hosts and remediate issues.	• Remediate critical issues that could allow unauthorized access to content within 48 hours. • Remediate non critical issues in a timely manner • Ensure that tools used for scanning/testing accommodate virtualization technologies, if being used • Consider having this performed by an independent third-party

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

No.	Security Topic	Best Practice	Implementation Guidance
DS-1.10	Firewall / WAN / Perimeter Security	Secure any point to point connections by using dedicated, private connections and / or encryption.	• Connections over the Internet or public networks should be encrypted using site-to-site VPN • Consider encrypting connections over private connections (e.g. dark fiber, leased lines, frame relay, MPLS, etc.) • Use advanced encryption standard (**AES256**) or higher for encryption • All point-to-point (e.g., VPN, private fiber, etc...) connections within the organization through which content travels should be documented and reviewed for usage and business validity at least every six months, three months recommended
DS-1.11	Firewall / WAN / Perimeter Security	Implement a synchronized time service protocol (e.g., Network Time Protocol) to ensure all systems have a common time reference.	• Ensure systems have the correct and consistent time • Ensure time data is protected • Ensure time settings are received from industry-accepted time sources
DS-1.12	Firewall / WAN / Perimeter Security	Establish, document and implement baseline security requirements for WAN network infrastructure devices and services.	• Ensure system defaults that could create vulnerabilities are modified before being placed into production • Consider continuous monitoring to report compliance of infrastructure against security baselines

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

No.	Security Topic	Best Practice	Implementation Guidance
DS-2.0	Internet	Prohibit production network and all systems that process or store digital content from directly accessing the internet, including email. If a business case requires internet access from the production network or from systems that process or store digital content, only approved methods are allowed via use of a remote hosted application / desktop session.	• 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 anti-virus definition servers, patching servers, licensing servers (only when local licenses are not available), etc. • Proxy license servers hosted on production networks are allowed provided that outgoing requests to the Internet are via non-persistent connections (open during a maintenance window) via strict ACLs. Patches directly to production workstations are allowed same way (open during a maintenance window). • 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 email 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 Block the mapping of local drives, block USB mass storage, block mapping of printers, block copy and paste functions, and block the download/upload to the Internet gateway system from the production network • A KVM, A keyboard / video / mouse (KVM) solution to a machine with Internet access not connected to the production network, may also be considered Ensure that any physical ports on the KVM switch which are not in use are properly locked down.

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

No.	Security Topic	Best Practice	Implementation Guidance
DS-2.1	Internet	Implement email filtering software or appliances that block the following from **non-production networks**: • Potential phishing emails • Prohibited file attachments (e.g., Visual Basic scripts, executables, etc.) • File size restrictions limited to 30 MB • Known domains that are sources of malware or viruses	• Identify restricted content types for email attachments and email message body • Implement an email filtering solution and configure based on restricted content types
DS-2.2	Internet	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

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

No.	Security Topic	Best Practice	Implementation Guidance
DS-3.0	LAN / Internal Network	Isolate the **content / production network** from **non-production networks** (e.g., office network, **DMZ**, the internet 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., anti-virus 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 anti-virus definition servers, patching servers, content delivery servers, licensing servers (only when local licensing servers are not available), etc. • Implement **firewall rules** to deny all inbound traffic by default and explicitly allow specific systems and ports that require inbound transmission from designated content delivery servers. • Refer to DS-2.0 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** • Prohibit any production computer system from connecting to more than one network at a time • Prohibit content from being used or stored in non-production networks
DS-3.1	LAN / Internal Network	Restrict access to the **content / production** systems to authorized computing hardware.	• Consider using physical Ethernet cable locks to ensure that a network cable cannot be connected to an alternate/unauthorized device

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

No.	Security Topic	Best Practice	Implementation Guidance

DS-3.2	LAN / Internal Network	Restrict remote access to the **content / production network** to only approved personnel who require access to perform their job responsibilities.	• Prohibit direct remote access to the **content / production** network without the use of a bastion host model
			• A business case with an approval process should be provided prior to granting remote access. Things to consider:
			  ○ Persistent connections are permitted for remote access to service VLAN for explicitly authorized production access (e.g., render and transcoding queue management)
			  ○ Remote access accounts should not be shared
			  ○ Remote access should be limited to the fewest people possible
			  ○ The remote access user account list should be reviewed every 90 days at a minimum. Accounts that are no longer active should be disabled
			  ○ Upon termination, an employee remote access should be immediately disabled
			• Maintain a list of **company personnel** who are allowed remote access to the **content / production network**
			• Develop processes for management to review remote activity on monitor access to 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
			• In the event emergency remote access is required, implement the following:
			  • Use two-factor authentication, and preferably certificate based
			  • Block file transfer protocols including, FTP, SSH, IRC, IM
			  • **VPN** configuration must not allow split tunneling
			  • Utilize a Launchpad/bastion host model as an intermediate to connect to the production network

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

No.	Security Topic	Best Practice	Implementation Guidance
DS-3.3	LAN / Internal Network	Use switches/layer 3 devices to manage network traffic. Disable all unused **switch** ports on the **content / production** network to prevent access from unauthorized devices.	• Use an secure protocol for accessing management interfaces • Use device administrator credentials with strong passwords • Separate password for exec commands if supported by the device • Disable unused ports on switches • Implement MAC filtering • Implement network based access control, i.e. 802.1X • Enable logging • If layer 2 switches are still in use, ensure that a firewall, router, or other higher layer network communications device is providing network isolation / traffic control.
DS-3.4	LAN / Internal Network	Restrict the use of non-switched devices such as hubs and repeaters on the **content/production network** *(Re added)*	• Replace all hubs/repeats with switches or layer 3 devices *(Re added)*
DS-3.5	LAN / Internal Network	Prohibit bridging or dual-homed networking (physical network bridging) on computer systems between **content / production networks** and non-content / production networks.	• Systems should not have connectivity to the data I/O networks and **content / production networks** at the same time. • Systems that require connectivity to a like production and a metadata network (i.e. Stornext) are exempt from the bridging exclusion.
DS-3.6	LAN / Internal Network	Implement a network-based intrusion detection /prevention system (**IDS / IPS**) to protect the **content / production network**.	• Configure the network-based intrusion detection / prevention system **(IDS / IPS**) to alert on / prevent suspicious network activity • Subscribe to anti-virus/anti-malware for the **IDS / IPS** • Update attack signature definitions/policies and anti-virus/anti-malware on the **IDS / IPS** on at least a weekly basis • Log all activity and configuration changes for the **IDS / IPS** • Considering implementing host-based intrusion detection system software on all workstations

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

No.	Security Topic	Best Practice	Implementation Guidance
DS-3.7	LAN / Internal Network	Disable SNMP (Simple Network Management Protocol) if it is not in use. Use SNMPv3 or higher with strong passwords for community strings.	• Use an **ACL** that restricts access to the SNMP device so that only authorized management systems from trusted zones may be used to connect. • Community strings must be different from those used in login credentials of security administration accounts.
DS-3.8	LAN / Internal Network	Harden systems prior to placing them in the **LAN / Internal Network**.	• Refer to DS-1.5 for suggestions
DS-3.9	LAN / Internal Network	Conduct internal network vulnerability scans and remediate any issues, at least annually.	• Ensure that tools used for scanning accommodate virtualization technologies, if being used • Include the following: Production networks Non-Production networks Connected machines / devices Non-connected machines / devices
DS-3.10	LAN / Internal Network	Store local backups of local area network, SAN/NAS, devices, servers and workstations on a server in a secure internal network**.**	• Configure local area network devices to store backups of configuration files in a secure manner (e.g., encrypted using AES 256) on a secure internal network • Ensure that only authorized administrators have access to the storage location and the encrypted backups

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

No.	Security Topic	Best Practice	Implementation Guidance

DS-3.11	LAN/ Internal Network	DNS servers used in the production network should not allow connections to and from the Internet	• Consider setting up a dedicated DNS server on the production network, only used for production DNS
			• DNS resolution that requires Internet name resolution should be on a network segment separate from production
			• Connections between the production DNS and Internet accessible DNS server should be restricted
			• Harden DNS servers prior to deployment to include the following items:
			  ○ DNS servers only listen on specified IP addresses
			  ○ Disable recursive queries
			  ○ Configure servers to prevent DNS cache poisoning
			  ○ Access control is implemented to only allow authorized individuals to perform administrative tasks on the DNS server

DS-4.0	Wireless/WLAN	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** • Wireless network access cards (NICs) should be disconnected from production computers either physically, or via endpoint security policy (e.g. Active Directory Group Policy Object, etc.)

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

No.	Security Topic	Best Practice	Implementation Guidance

DS-4.1	Wireless/WLAN	Configure **non-production** wireless networks (e.g., administrative and guest) with the following security controls:
		
		• Disable WEP / WPA
		• Enable **WPA2-PSK (AES)**
		• Segregate "guest" networks from the company's other networks
		• Change default administrator logon credentials
		• Change default network name (**SSID**)
			• Consider additional security controls such as:
			  • Use non-company, non-production, specific **SSID** names
			  • RADIUS for authentication where the option is available
			  • WPA2-Enterprise (AES) if applicable
			  • **MAC address filtering**
			  • Blacklist the wireless MAC addresses of production workstations and devices
			  • Configure the wireless access point / controller to broadcast only within the required range
			• Consider implementing port based network access control (e.g. 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
			• Implement the following controls if pre-shared keys must be used:
			  • Configure WPA2 with CCMP (**AES**)
			  • Set a complex passphrase (See DS-8.1 for passphrase complexity recommendations)
			  • Change the passphrase at least every 90 days and when key **company personnel** terminate their employment

DS-4.2	Wireless/WLAN	Implement a process to scan for rogue wireless access points and remediate any validated issues.	• Implement a process to roam and scan the facility for unprotected wireless access points at least quarterly • Configure a centralized wireless access solution (i.e., wireless controller) to alert administrators of rogue wireless access points upon detection, if possible

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

No.	Security Topic	Best Practice	Implementation Guidance
DS-5.0	I/O Device Security	Designate specific data I/O systems to be used for uploading / downloading content from / to external networks (Internet).	• Implement **ACLs** to allow traffic between the **content / production network** and systems used for I/O for specific source/destination **IP addresses** • Implement whitelisting to restrict content downloads and uploads to only authorized external sources and destinations

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

DS-5.0.1	I/O Device Security	Implement a multi-layered network architecture for ingesting content from external networks (Internet) into the production network, and moving content from the production network to external networks.	• Implement separate isolated networks for data I/O and production. • Use dedicated data I/O workstations to move content between external networks (Internet) and inbox / outbox storage. • Inbox / outbox storage should be local to data I/O workstations or located in data I/O network • Use a separate set of credentials, one for the data I/O side, and another for the production side to access the inbox/outbox storage • Data movement must be initiated from the more secure layer: i.e. push / pull content at the data I/O zone to / from Internet; push / pull content at the production network to / from the data IO zone • Accordingly, implement strict (IP and port) layer 2/3 ACLs to allow outbound network requests from the more trusted inner layer, and deny all inbound requests from the less trusted outer layers • Delete content after it is moved from the inbox / outbox storage. Consider the use of scripts to automatically delete content in the inbox / outbox storage after it has been there for a certain period of time, e.g. 24-48 hours. • For facilities with sufficient resources, consider stronger separation of duties: requiring two different sets of individuals, one on production side, and one on data I/O side, to move content from production to external networks. • Exceptions: Use of separate volumes for the inbox / outbox storage on the same SAN used for production is allowed if access to the data IO and production volumes can be restricted via layer 2/3 ACLs (Isilon, NetApp, etc.) Other secure implementations may exist: e.g. dedicated inbox / outbox storage located in the production network, but only accessible from the data I/O network

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

No.	Security Topic	Best Practice	Implementation Guidance
			via a SMB proxy server that communicates across networks via strict layer 2/3 ACLs Obtain client approval for other exceptions.
DS-5.1	I/O Device Security	Block input/output (I/O), mass storage, external storage, and mobile storage devices (e.g., **USB**, **FireWire**, Thunderbolt, SATA, **SCSI**, etc.) and optical media burners (e.g., DVD, Blu-Ray, CD, etc.) on all systems that handle or store content, with the exception of systems used for content I/O. Refer to DS-4.0 for disconnecting wireless NICs.	• 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 • Write access to external devices is allowed if there is a valid business justification. Computers that allow write-access to external devices must utilize an I/O port monitoring and logging solution.
DS-6.0	System Security	Install anti-virus and anti-malware software on all workstations, servers, and on any device that connects to SAN/NAS systems.	• Install an enterprise anti-virus and anti-malware solution with a centralized management console • Consider the installation of endpoint protection
DS-6.1	System Security	Update all anti-virus and anti-malware definitions daily, or more frequently.	• Configure the centralized anti-virus and anti-malware management console to download and push definition updates at least once each day
DS-6.2	System Security	Scan all content for viruses and malware prior to ingest onto the **content / production network**.	• Perform scans on a system that is not connected to the **content / production network** • To avoid impact on content / production systems, configure anti-virus and anti-malware software to only execute full file system scans during idle hours, non-business hours, and/or weekends.
DS-6.2.1	System Security	Local firewalls should be implemented on workstations to restrict unauthorized access to the workstation.	• Consider implementing on machines with higher security requirements that might also have access to the Internet (e.g. I/O machines, workstations used for Internet research etc.)

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

No.	Security Topic	Best Practice	Implementation Guidance
DS-6.3	System Security	Perform scans as follows: • Enable regular full system virus and malware scanning on all workstations • Enable full system virus and malware scans for servers and for systems connecting to a SAN/NAS	• Configure anti-virus and anti-malware software to conduct a full system scan based upon the anti-virus and anti-malware strategy • Configure anti-virus and anti-malware software to execute during idle periods
DS-6.4	System Security	Implement a process to regularly update systems (e.g., file transfer systems, operating systems, databases, applications, network devices) with patches/updates that remediate security vulnerabilities.	• Where possible, implement a centralized patch management tool (e.g., WSUS, Shavlik, Altiris) to automatically deploy patches to all systems • Subscribe to security and patch notifications from vendors, other third parties, and security advisories • Apply critical patches as soon as they become available and within 48 hours on computers on externally accessible networks • Apply less critical patches in a timely manner, according to a defined cycle based on risk (e.g. monthly for medium, quarterly for low, etc.) • Test patches prior to deployment • Decommission legacy systems that are no longer supported • Implement an exception process and compensating controls for cases where there is a legitimate business case for not patching systems
DS-6.5	System Security	Prohibit users from being Administrators on their own workstations, unless required for software (e.g., ProTools, Clipster and authoring software such as Blu-Print, Scenarist and Toshiba). Documentation from the software provider must explicitly state that administrative rights are required.	• Ensure that the user account used to login to the workstation does not have privileges as an Administrator of the system
DS-6.6	System Security	Use cable locks on transportable computing devices that handle content (e.g., laptops, tablets, desktops, towers) when they are left unattended.	• Secure cable lock to a stationary object (e.g., table)

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

No.	Security Topic	Best Practice	Implementation Guidance
DS-6.6.1	System Security	Apply seals or tamper evident stickers on cases used for all workstations and servers that receive, send, manipulate, or store content in the production network	• E.g. Data IO machines, to help secure the machines from physical tampering.
DS-6.7	System Security	Implement additional security controls for laptops and portable computing storage devices that contain content or sensitive information relating to client projects. Encrypt all laptops. Use hardware-encrypted portable computing storage devices. Install remote-kill software on all laptops/mobile devices that handle content to allow remote wiping of hard drives and other storage devices.	• Attach privacy screens to laptops if they must be used in insecure locations • Do not connect laptops to any public wireless locations • Power down laptops when not in use, and do not make use of sleep or hibernation modes
DS-6.8	System Security	Restrict software installation privileges to IT management.	• Prohibit the installation and usage of unapproved software including rogue software (e.g., illegal or malicious software) • Scan all systems for an inventory of installed applications at least quarterly
DS-6.9	System Security	Implement security baselines and standards to configure systems (e.g., laptops, workstations, servers, SAN/NAS) that are set up internally.	• Develop a secure standard build that is used to image all systems
DS-6.10	System Security	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
DS-6.11	System Security	Maintain an inventory of systems and system components.	• Update the inventory on at least a monthly basis
DS-6.12	System Security	Document the network topology and update the diagram annually or when significant changes are made to the infrastructure.	• Include WAN, DMZ, LAN, WLAN (wireless), VLAN, firewalls, and server/network topology

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

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 Disallow the sharing of any user account by multiple users Restrict the use of service accounts to only applications that require them • 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 including **VPN**) Production operating systems Content management components (e.g., storage devices, content servers, content storage tools, content transport tools) Systems with Internet access Implement a server to manage the logs in a central repository (e.g., syslog/log management server, Security Information and Event Management (**SIEM**) tool)
DS-7.1	Account Management	Maintain traceable evidence of the account management activities (e.g., approval emails, change request forms).	• Retain evidence of management approvals and associated actions for all account management activities, where possible

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

No.	Security Topic	Best Practice	Implementation Guidance
DS-7.2	Account Management	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, Open Directory, LDAP) **VPN** remote permissions, which should only be granted when absolutely required
DS-7.3	Account Management	Rename the default administrator accounts and other default 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
DS-7.4	Account Management	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

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

No.	Security Topic	Best Practice	Implementation Guidance
DS-7.5	Account Management	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-7.6	Account Management	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**. Review user access on the following: Key applications (content management, inventory, etc.) Project folders, data I/O inbox / outbox, and centralized storage Network communications devices (firewalls, routers, switches, etc.) • Change shared account (administrator, root) passwords when persons who know those passwords no longer require access • Remove or disable accounts that have not been used in over 90 days
DS-7.7	Account Management	Restrict 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

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

No.	Security Topic	Best Practice	Implementation Guidance
DS-7.8	Account Management	Disable or remove local accounts on systems that handle content where technically feasible.	• 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 • Disable the guest account • If local accounts must be used, where possible, change the user name and password for each default account, disable the ability to logon to the system through the network using local accounts
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

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

DS-8.1	Authentication	Enforce a strong password policy for gaining access to **information systems**. Password policy should include guidance for service accounts.	A facility should opt to choose one or more of the following password policies (A to C, listed in order of most preferred) for user accounts for employees, guests, contractors, and/or vendors: A) Utilize **multi-factor authentication (MFA)** that uses a combination of two or more the following: 1. Something they know and only they know (e.g. password) 2. Something they have and only they have (e.g. soft or hard token) 3. Something they and only they are (e.g. biometrics) B) Password policies that are able to demonstrate the implementation of all the following criteria based on NIST 800-63b: 1. Password length is at least 12 characters 2. Passwords cannot contain common names or dictionary names (e.g. password1234, companyname!, firstnamelastname1) and should be enforced via a password black list 3. Password lockout must occur after 5 invalid attempts and can be automatically locked out after 1 minute 4. A manual password reset must require the password to be changed after the next successful login 5. All passwords hashes are reviewed quarterly for weaknesses via password cracking tools 6. Hashes are run through cracking tools for a minimum of 24 hours 7. The password black list is updated quarterly 8. Passwords that are cracked must be added to the black list and changed within 30 days C) Create a password policy that consists of the following: 1. Minimum password length of 12 characters 2. Minimum of 3 of the following parameters: upper case, lower case, numeric, and special characters 3. Maximum password age of 365 days 4. Minimum password age of 1 day 5. Maximum invalid logon attempts of between 3 and 5 attempts 6. User accounts locked after invalid logon attempts must be manually unlocked, and should not automatically unlock after a certain amount of time has passed 7. Password history of ten previous passwords D) **Service accounts** unable to comply with A) to C) should adhere to the following criteria at a minimum: 1. Restrict access to only what is needed for services 2. Minimum password length of 12 characters 3. Minimum of 3 of the following parameters: upper case, lower case, numeric, and special characters 4. Maximum invalid logon attempts of between 3 and 5 attempts 5. Monitoring and alerts of the following activities via central logging: i. Successful login ii. Failed logon due to bad password or user name iii. Failed logon due to account lockout iv. Failed logon due to inadequate rights v. Review of activity on a monthly basis vi. Changing of passwords upon detection of suspicious activity • Consider the use of a **Privileged Account Management (PAM**) tool

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

DS-8.2	Authentication	For remote access (e.g., **VPN**) to the networks, implement two-factor authentication (e.g., username / password and hard token) and monitor activity.	• Require individuals to provide two of the following for remote access: Information that the individual knows (e.g., username, password) A unique physical item that the individual has (e.g., token, **keycard**, smartphone, certificate) A unique physical quality/biometrics that is unique to the individual (e.g., fingerprint, retina) • Use two-factor authentication and a **VPN** connection with advanced encryption standard (**AES-256**) to carryout remote administration functions • Review remote access VPN logins and activity on at least a monthly a basis
DS-8.2.1	Authentication	Implement two-factor authentication (e.g., username / password and hard token / verification code text message) for access to web based e-mail (Google, Microsoft, etc.) from desktops or mobile computing devices.	• If smartphone access to e-mail s ~~is~~ not necessary, consider blocking webmail from smartphones to force desktop access • Do not use personal accounts - use corporate accounts on enterprise offerings • Web based e-mail services should have virus and malware protection
DS-8.3	Authentication	Implement password-protected screensavers or screen-lock software 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
DS-8.4	Authentication	Consider implementing additional authentication mechanisms to provide a layered authentication strategy for WAN and LAN / Internal Network access.	• Consider adding one or more of the following: Multi-factor authentication Identity and access management system Single sign on system Identity federation standards

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

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 (e.g., **VPN** systems) Production operating systems Content management components (e.g., storage devices, content servers, content storage tools, content transport tools) Systems with Internet access Applications
DS-9.01	Logging and Monitoring	Implement logging mechanisms on all systems used for the following: • Key generation • **Key management** • Vendor certificate management	• Ensure that all generated keys and added certificates are traceable to a unique user
DS-9.1	Logging and Monitoring	Implement a server to manage the logs in a central repository (e.g., syslog/log management server, Security Information and Event Management (**SIEM**) tool).	
DS-9.2	Logging and Monitoring	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 Attempts at privilege escalation • Implement a server to aggregate logs in a central repository (e.g., syslog/log management server, Security Information and Event Management (**SIEM**) tool)
DS-9.3	Logging and Monitoring	Investigate any unusual activity reported by the logging and reporting systems.	• Incorporate **incident response** procedures for handling detected security events

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

DS-9.4	Logging and Monitoring	Review all logs weekly, and review all critical and high daily.	• 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 • Based on findings of log reviews, update **SIEM** settings as appropriate
DS-9.5	Logging and Monitoring	Enable logging of internal and external content movement and 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-9.6	Logging and Monitoring	Retain logs for at least one year.	• 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

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

DS-9.7	Logging and Monitoring	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-10.0	Mobile Security	Define security controls and standards for mobile computing devices. Refer to MS-4.0.2 for mobile computing device policies.	• Consider implementing the following mobile computing device security controls and standards: antivirus/anti-malware protection inactivity lock (PIN, swipe, fingerprint) data wipe after successive invalid attempts to unlock data encryption patching and OS revision management remote data wipe centralized mobile device management approved models
DS-10.1	Mobile Security	Develop a list of approved applications, application stores, and application plugins/extensions for mobile devices accessing or storing content.	• Prohibit the installation of non-approved applications or approved applications that were not obtained through a pre-approved application store • Consider a mobile device management system
DS-10.2	Mobile Security	Maintain an inventory of all mobile devices that access or store content.	• Include operating system, patch levels, applications installed
DS-10.3	Mobile Security	Require encryption either for the entire device or for areas of the device where content will be handled or stored.	• Consider a mobile device management system
DS-10.4	Mobile Security	Prevent the circumvention of security controls.	• Prevent the use of jailbreaking, rooting etc.
DS-10.5	Mobile Security	Implement a system to perform a remote wipe of a mobile device, should it be lost / stolen / compromised or otherwise necessary.	• Remind employees that non-company data may be lost in the event a remote wipe of a device is performed
DS-10.6	Mobile Security	Implement automatic locking of the device after 10 minutes of non-use.	

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

DS-10.7	Mobile Security	Manage all mobile device operating system patches and application updates.	• Apply the latest available security-related patches/updates upon general release by the device manufacturer, carrier or developer
DS-10.8	Mobile Security	Enforce password policies.	• Refer to DS-8.1 • Use biometrics (fingerprint reader)
DS-10.9	Mobile Security	Consider implementing a system to perform backup and restoration of mobile devices.	• Encrypt backups and store them in a secure location

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

No.	Security Topic	Best Practice	Implementation Guidance
DS-11.0	Security Techniques	Ensure that security techniques (e.g., spoiling, invisible/visible **watermarking**) are available for use and are applied when instructed.	

DS-11.1	Security Techniques	Encrypt content on hard drives or encrypt entire hard drives using a minimum of **AES-256 encryption** by either:
		• File-based **encryption**: (i.e., encrypting the content itself)
		• Drive-based **encryption**: (i.e., encrypting the hard drive)
			• For external hard drives, consider purchasing pre-encrypted drives (e.g., Rocstor Rocsafe, LaCie Rugged Safe, Apricorn)
			• The use of external hard drives should be approved by the client prior to use.
			
			Single factor authentication is allowed only if the authentication is a keypad pin. Without a keypad pin authentication, consider using client approved encryption solutions.
			
			Drives with keypad pin authentication should enforce limited invalid authentication attempts after which content stored on the drives is erased or the drives self-destruct.
			
			• Encrypt all content on hard drives including:
			  • SAN / NAS
			  • Servers
			  • Workstations
			  • Desktops
			  • Laptops
			  • Mobile devices
			  • External storage drives
			• Implement one or more of the following:
			  • File-based **encryption** such as encrypted DMGs or encrypted ZIP files
			  • Drive-based **encryption** using software

DS-11.2	Security Techniques	Send decryption keys, keypad pins, 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	FACILITY	ASSET MANAGEMENT	TRANSPORT	INFRASTRUCTURE	CONTENT MANAGEMENT	CONTENT TRANSFER

No.	Security Topic	Best Practice	Implementation Guidance
DS-11.3	Security Techniques	Implement and document key management policies and procedures: • Use of encryption protocols for the protection of sensitive content or data, regardless of its location (e.g., servers, databases, workstations, laptops, mobile devices, data in transit, email) • Approval and revocation of trusted devices • Generation, renewal, and revocation of content keys • Internal and external distribution of content keys • Bind encryption keys to identifiable owners • Segregate duties to separate key management from key usage • Key storage procedures • Key backup procedures	• Consider the creation of unique encryption keys per client and for critical assets • Prevent unauthorized substitution of cryptographic keys • Require cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities
DS-11.4	Security Techniques	Encrypt content at rest and in motion, including across virtual server instances, using a minimum of **AES-256 encryption**.	• http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf
DS-11.5	Security Techniques	Store secret and private keys (not public keys) used to encrypt data/content in one or more of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (e.g., Host Security Module (HSM) or a Pin Transaction Security (PTS) point-of-interaction device) Has at least two full-length key components or key shares, in accordance with a security industry accepted method	
DS-11.6	Security Techniques	Confirm that devices on the **Trusted Devices List (TDL)** are appropriate based on rights owners' approval.	• Require clients to provide a list of devices that are trusted for content playback • Only create Key Delivery Messages (KDMs) for devices on the **TDL**

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

No.	Security Topic	Best Practice	Implementation Guidance
DS-11.6.1	Security Techniques	Access to KDMs must be restricted to the KDM creator and exhibitor only.	
DS-11.6.2	Security Techniques	KDM creation and handling must be physically and digitally segregated from DCP handling and replication where feasible.	
DS-11.7	Security Techniques	Confirm the validity of content keys and ensure that expiration dates conform to client instructions.	• Require clients to provide expiration dates for content keys • Specify an end date for when keys expire to limit the amount of time for which content can be viewed
DS-12.0	Content Tracking	Implement a digital content management system to provide detailed tracking of digital content.	• Log all digital content that is checked-in/checked-out • Log the digital location of all content • Log the expected duration of each check-out • Log the time and date of each transaction
DS-12.1	Content Tracking	Retain digital content movement transaction logs for one year.	• Include the following: Time and date of check-in/check-out Name and unique id of the individual who checked out an asset Reason for check-out Location of content
DS-12.2	Content Tracking	Review logs from digital content management system periodically and investigate anomalies.	
DS-12.3	Content Tracking	Use client AKAs (“aliases”) in asset tracking systems, unless otherwise as directed by the client.	• Restrict knowledge of client AKAs to personnel involved in processing client assets
DS-12.4	Content Tracking	Use enterprise (not personal) versions of online or web based collaboration services (e.g., Google Docs, etc.) for tracking content, managing inventory, or workflow management, Utilize multi-factor authentication and centrally managed user accounts and access to data.	• Implement two-factor authentication • Subscribe to enterprise or corporate editions to allow centralized management of users and access to data • Review user accounts and access to data and files on a quarterly basis (refer to DS-7.6) • Implement a periodic process to purge old data and files

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

No.	Security Topic	Best Practice	Implementation Guidance
DS-13.0	Transfer Systems	Use only client-approved **transfer** systems that utilize access controls, a minimum of **AES-256** encryption for content at rest and for content in motion and use strong authentication for content transfer sessions.	• Allow only authorized users to have access to the content transfer system • Consider restricting access also on a project basis • Verify with the client that the content transfer systems are approved, prior to use
DS-13.1	Transfer Systems	Implement an exception process, where prior client approval must be obtained in writing, to address situations where encrypted **transfer tools** are not used.	• Use randomly generated usernames and passwords that are securely communicated for authentication • Use only client-approved transfer tools / application • Require clients to sign off on exceptions where unencrypted **transfer tools** must be used • Document and archive all exceptions
DS-14.0	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 • Disable **VPN**/remote access to transfer systems, or to any system used to store, transfer or manipulate content
DS-14.1	Transfer Device Methodology	Separate content transfer systems from administrative and production networks.	• Separate networks either physically or logically
DS-14.2	Transfer Device Methodology	Place content transfer systems in a **Demilitarized Zone** (**DMZ**) and not in the **content / production network**. Implement whitelisting on content transfer servers to only allow transfers to and from authorized external transfer servers.	• Harden content transfer systems prior to placing them in the **DMZ** (refer to DS-1.5 for suggestions) • 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** • Disable access to the Internet from the systems used to transfer content, other than the access needed to download client content or to access approved content transfer locations • Review and update white listings quarterly

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

No.	Security Topic	Best Practice	Implementation Guidance
DS-14.3	Transfer Device Methodology	Remove content from content transfer devices/systems immediately after successful transmission/receipt.	• Require clients to provide notification upon receipt of content • Implement a process to remove content from transfer devices and systems, including from recycle bins • Where applicable, remove client access to **transfer tools** immediately after project completion • Confirm the connection is terminated after the session ends
DS-14.4	Transfer Device Methodology	Send automatic notifications to the production coordinator(s) upon outbound content transmission.	• Configure the content transfer system to send an automatic notification (e.g., an email) to the production coordinator(s) each time a user sends content out of the network
DS-15.0	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 Manage encryption keys using proper segregation of duties (e.g., one person should create the keys and another person should use the keys to encrypt the content) 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

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

No.	Security Topic	Best Practice	Implementation Guidance
DS-15.1	Client Portal	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 emails • Consider distributing user credentials via phone or SMS • Consider distributing encryption keys via out of band transfer • Create a password policy that consists of the following: Refer to DS-8.1 for details
DS-15.2	Client Portal	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 at least quarterly • Ensure that access is restricted to only those that require it
DS-15.3	Client Portal	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** • Harden systems prior to placing them in the **DMZ** (refer to DS-1.5 for suggestions)
DS-15.4	Client Portal	Prohibit the use of third-party production software/systems/services that are hosted on an internet web server unless approved by client in advance.	• Consider adding one or more of the following: Multi-factor authentication Identity and access management system Single sign on system Identity federation standards Use a **VPN** connection with advanced encryption standard (**AES-256)**
DS-15.5	Client Portal	Use **HTTPS** and enforce use of a strong cipher suite (e.g., TLS v1.3) for the internal/external web portal. Acquire an **HTTPS** public key certificate signed by a certificate authority trusted by a majority of web browsers.	• Ensure certificates are up to date and not expired • Avoid the use of self-signed certificates

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

No.	Security Topic	Best Practice	Implementation Guidance
DS-15.6	Client Portal	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-15.7	Client Portal	Set access to content on internal or external portals to expire automatically at predefined intervals, where configurable.	
DS-15.8	Client Portal	Test for web application vulnerabilities quarterly and remediate any validated issues.	• 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) • Testing should be performed by an independent third party
DS-15.9	Client Portal	Perform annual penetration testing of web applications and remediate any validated issues.	• 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) • Testing should be performed by an independent third party
DS-15.10	Client Portal	Allow only authorized personnel to request the establishment of a connection with the telecom service provider.	
DS-15.11	Client Portal	Prohibit transmission of content using email (including webmail).	• Consider the use of secure email appliance servers to encrypt emails and attachments (e.g., Cisco IronPort, Sophos E-Mail Security Appliance, Symantec PGP Universal Gateway Email)

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

No.	Security Topic	Best Practice	Implementation Guidance
DS-15.12	Client Portal	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 • Consider sending automatic email notifications to an appropriate party whenever data is transferred
DS-15.13	Client Portal	Implement a process to review the facility's public informational website and other online industry resources for sensitive information that could be leveraged by an attacker (e.g. mentions of internal infrastructure and technologies, content transfer servers, IP addresses, photos of sensitive areas, current content being worked on, etc.)	• Implement a change control / approval process and/or tool before content can be added to or modified on the public informational website. • Review IMDb, LinkedIn, etc.

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.
Content/ Production Network	A computer network that is used to store, transfer, or process media content.

Term or Acronym	Description
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 cipher text, which cannot be easily understood by unauthorized people.
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.

Term or Acronym	Description
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.
HTTPS	A communications protocol for secure communication over a computer network, with especially wide deployment on the Internet.
Identification Badge	Card used to identify individuals authorized to access a facility (e.g., employees, vendors, visitors).
IP Camera	A digital video camera used as part of an IP Camera surveillance system.
Intrusion Detection/ Intrusion Prevention (IDS/IPS)	An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. An intrusion prevention system (IPS) performs the same function and also attempts to block the activity.
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).

Term or Acronym	Description
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.
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.
Multi-Factor Authentication (MFA)	Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric) (Reference NIST 800-54 Rev. 4). **Note**: MFA could also be known as “Two-Factor” (2FA).

Term or Acronym	Description
Network Protocol	Convention or standard that controls or enables the connection, communication, and data transfer between computing endpoints.
Network Video Recorder (NVR)	A video recorder used to record IP camera video footage
Network Interface Card (NIC)	A computer hardware component that connects a computer to a computer network.
Penetration Testing	Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability (source: NIST SP 800-115). **Note:** A vulnerability scan alone does not always suffice as a penetration test.
Privileged Account Management (PAM)	Privileged account management (PAM) is a domain within identity and access management (IdAM) that focuses on monitoring and controlling the use of privileged accounts. Privileged accounts include local and domain administrative accounts, emergency accounts, application management, and **service accounts** (source: NIST SP-1800-18)

Term or Acronym	Description
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.
Security information and event management (SIEM)	A term for software products and services combining security information management (SIM) and security event management (SEM). SIEM technology provides real-time analysis of security alerts generated by network hardware and applications
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.
Service Account	A service account is an account that a service on your computer uses to run under and access resources. This should not be a user's personal account. A service account could also be an account that is used for a scheduled task (sometimes referred to as a batch job account), or an account that is used in a script that is run outside of a specific user's context. (source: SANS "Securing Windows Service Accounts")

Term or Acronym	Description
Service Set Identifier (SSID)	A unique identifier for a wireless LAN, which is often a human-readable string and thus commonly called the "network name".
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.
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.

Term or Acronym	Description
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 / Internal Network but not limited to physical location.
Virtual Private Network (VPN)	Computer network that allows users to access another larger network.
Vulnerability Scans	A technique used to identify hosts/host attributes and associated vulnerabilities (source: NIST SP 800-115). **Note:** A vulnerability scan alone does not suffice as a penetration test. Refer to the **Penetration Testing** definition for details.
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 MPA TITLE AND DISTRIBUTION CHANNEL DEFINITIONS

Title Types

<table>
<tr><th>Title Type</th><th>Description</th></tr>
<tr><td>Feature</td><td>A type of work released theatrically or direct to home video or to Internet that includes the following types:
<table>
<tr><th>Feature Type</th><th>Description</th></tr>
<tr><td>Feature Film</td><td>A full length movie.</td></tr>
<tr><td>Short</td><td>A film of length shorter than would be considered a feature film.</td></tr>
<tr><td>Long-Form Non-Feature</td><td>Other works, for example, a documentary.</td></tr>
</table></td></tr>
<tr><td>TV Episodic</td><td>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”).</td></tr>
<tr><td>TV Non-Episodic</td><td>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).</td></tr>
<tr><td>Promotion / Advertisement</td><td>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’.</td></tr>
</table>

<table>
<tr><th>Title Type</th><th>Description</th></tr>
<tr><td>Ad</td><td>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.</td></tr>
<tr><td>Music</td><td>A type of work that includes ringtone, music videos and other music.</td></tr>
<tr><td>Other</td><td>A type of work that includes:
<table>
<tr><th>Type</th><th>Description</th></tr>
<tr><td>Excerpt</td><td>An asset that consists primarily of portion or portions of another work or works.</td></tr>
<tr><td>Supplemental</td><td>Material designed to supplement another work. For example, an extra associated with a DVD.</td></tr>
<tr><td>Collection</td><td>A collection of assets not falling into another category. For example, a collection of movies.</td></tr>
<tr><td>Franchise</td><td>A collection or combination of other types, for example, a franchise might include multiple TV shows, or TV shows and movies.</td></tr>
</table></td></tr>
</table>

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.

Distribution Channel	Description
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 -2013 Reference	NIST 800-53 Rev. 4 Reference
MS-1.0	Executive Security Awareness/ Oversight	6.1.1	PM-1, PM-2
MS-1.1		6.1.1	AT-2, AT-3, PM-1, PM-2
MS-1.2		5.1.2, 6.1.1	PM-1, PM-6, AT-3
MS-1.3		5.1.2, 6.1.1	PM-1, PM-6, AT-3
MS-2.0	Risk Management	6.1.1	CA-1, RA-1
MS-2.1		5.1.2	RA-2
MS-3.0	Security Organization	6.1.3	PM-2
MS-4.0	Policies and Procedures	5.1.1, 6.1.1	PL-1
MS-4.1		5.1.2	PL-1
MS-4.2		8.1.3	PL-1, PS-7
MS-4.3		8.2.2, 8.1.3	AT-1, AT-2, AT-3, AT-4
MS-5.0	Incident Response	16.1.1	IR-1, IR-8
MS-5.1			IR-2
MS-5.2		16.1.2	IR-6, IR-7
MS-5.3		16.1.2	IR-4, IR-5
MS-6.0	Business Continuity & Disaster Recovery	17.1.1	CP
MS-6.1		17.1.1	CP

No.	Security Topic	ISO 27002 -2013 Reference	NIST 800-53 Rev. 4 Reference
MS-7.0	Change Control & Configuration Management	14.2.2	CM
MS-8.0	Workflow	11.1	
MS-8.1		11.1	
MS-9.0	Segregation of Duties	6.1.2	AC-5
MS-10.0	Background Checks	7.1.1	PS-3
MS-11.0	Confidentiality Agreements	7.1.2	PL-4, PS-6, SA-9
MS-11.1		8.1.4	PS-4, PS-8
MS-12.0	Third Party Use and Screening	7.1.2	PL-4, PS-6, SA-9
MS-12.1		8.1.4	PS-7, SA-9
MS-12.2		7.2.1	PS-4
MS-12.3		8.14	
MS-12.4		7.1.2	PS-7
MS-12.5		11.1.2	PL-4, PS-6, SA-9
MS-12.6		7.1.1	
PS-1.0	Entry/Exit Points	11.1	PE-3
PS-1.1		11.1	PE-3, PE-6
PS-1.2		11.1	PE-1, PE-2, PE-3

No.	Security Topic	ISO 27002 -2013 Reference	NIST 800-53 Rev. 4 Reference
PS-2.0	Visitor Entry/Exit	11.1	PE-8
PS-2.1		11.1	PE-7, PE-2, PE-3
PS-2.2		11.1	PE-3
PS-2.3		11.1	PE-7, PE-2, PE-3
PS-3.0	Identification	11.1.2	PE-3
PS-4.0	Perimeter Security	11.1.1	PE-3
PS-4.1		11.1.1	PE-3
PS-4.2		11.1.1	PE-3
PS-4.3		11.1.1	PE-3
PS-5.0	Alarms	11.1.1	PE-3, PE-6
PS-5.1			PE-6
PS-5.2		11.1.1	AC-6
PS-5.3		11.1.1	
PS-5.4		11.1.1	PE-3, PE-6
PS-5.5		11.1.1	PE-3
PS-5.6		11.1.1	PE-6
PS-5.7		11.1.1	PE-9, PE-10, PE-11, PE-13
PS-6.0	Authorization	11.1	PE-1, PE-2, PE-3
PS-6.1		11.1	PE-2,
PS-6.2		11.1	PE-2, PS-4, PS-5
PS-7.0	Electronic Access Control	11.1	PE-2, PE-3
PS-7.1		11.1	PE-2, PE-3
PS-7.2		11.1	PE-2, PE-3
PS-7.3		11.1	PE-2, PE-3
PS-7.4		11.1	PE-2, PE-3

No.	Security Topic	ISO 27002 -2013 Reference	NIST 800-53 Rev. 4 Reference
PS-8.0	Keys	11.1	PE-2, PE-3
PS-8.1		11.1	PE-2, PE-3
PS-8.2		11.1	PE-2, PE-3
PS-8.3		11.1	CM-8
PS-8.4		9.2.6	CM-5, CM-8
PS-8.5		9.2.6	CM-5, CM-8
PS-9.0	Cameras		PE-6
PS-9.1		11.1	PE-6
PS-9.2		11.1	PE-2, PE-3
PS-9.3		11.1	AU-6, PE-6
PS-9.4		11.1	PE-6
PS-10.0	Logging and Monitoring	12.4	AU-3, AU-6 AU-9, AU-11
PS-10.1		12.4	AU-6
PS-10.2		12.4	AU-6
PS-11.0	Searches	11.1	
PS-11.1			
PS-11.2			
PS-11.3			
PS-11.4			
PS-11.5			
PS-11.6		11.1	
PS-11.7			
PS-11.8			
PS-11.9			
PS-12.0	Inventory Tracking	8.1	CM-8

No.	Security Topic	ISO 27002 -2013 Reference	NIST 800-53 Rev. 4 Reference
PS-12.1		8.2.2	MP-3
PS-12.2		8.2.3	AU-9, AU-11
PS-12.3			AU-6, CM-8
PS-12.4			
PS-12.5		8.2.3	AU-1, AU-3, AU-6
PS-12.6		8.2.3	
PS-13.0	Inventory Counts	8.1.1	AU-6, CM-8
PS-13.1		6.1.2	AC-5
PS-14.0	Blank Media/ Raw Stock Tracking	8.2.2	MP-4
PS-14.1		8.1.1	MP-4, PE-2, PE-3
PS-14.2			
PS-15.0	Client Assets	8.2.3	MP-4, PE-2, PE-3
PS-15.1		8.2.3	MP-2, MP-4
PS-15.2			
PS-15.3			
PS-15.4			
PS-16.0	Disposals	8.3.2	MP-6
PS-16.1		8.3.2	MP-6
PS-16.2			MP-6
PS-16.3			MP-6
PS-16.4			
PS-17.0	Shipping	8.3.3	MP-5
PS-17.1		8.3.3	AU-11, PE-16, MP-5
PS-17.2		8.2.3	MP-5
PS-17.3		8.3.3	PE-3, PE-7
PS-17.4		8.3.3	PE-3, PE-7
PS-17.5			
PS-17.6			
PS-17.7			
PS-17.8			
PS-17.9			
PS-18.0	Receiving	8.2.3	PE-16
PS-18.1			MP-5
PS-18.2		8.2.2	MP-3, MP-4
PS-18.3		8.2.3	MP-3, MP-5
PS-19.0	Labeling	8.2.2	MP-3
PS-20.0	Packaging	8.3.3	MP-5
PS-20.1		8.3.3	
PS-20.2			
PS-21.0	Transport Vehicles		MP-5
PS-21.1			
PS-21.2			
PS-21.3			
DS-1.0	External Network/WAN	13.1	AC-4, SC-7
DS-1.1		9.1, 13.1, 13.2	AC-3, AC-4
DS-1.2		10.1, 13.2	CM-7
DS-1.3		13.2	AC-20, CA-3, SC-7
DS-1.4		12.6	CM-6, SI-2
DS-1.5			CM-6, CM-7
DS-1.6		9.4, 10.1	AC-6, AC-17
DS-1.7		12.3, 17.1	
DS-1.8		12.6, 13.1	RA-5, SC-7

No.	Security Topic	ISO 27002 -2013 Reference	NIST 800-53 Rev. 4 Reference
DS-1.9		12.6	RA-5, SC-7
DS-1.10		10.1, 13.1	SC-7, SC-12, SC-33
DS-1.11		12.4	SC-7, SC-12, SC-33
DS-1.12		12.2, 16.1	SC-7, SC-12, SC-33
DS-2.0	Internet	12.1, 13.1	CA-3
DS-2.1		13.2	PL-4
DS-2.2		13	AC-6, PL-4
DS-3.0	LAN/Internal Network	9.4, 13.1	SC-7
DS-3.1		11.2	
DS-3.2		6.2, 13.1, 9	AC-3, AC-17
DS-3.3		10.1	CM-6, CM-7
DS-3.4		13.1	SC
DS-3.5		13.1	SC
DS-3.6		16.1	SI-4
DS-3.7		9.4	SC
DS-3.8		9.1	SC
DS-3.9		12.6	SC
DS-3.10		12.3, 17.1	SC
DS-4.0	Wireless	9.1, 13.1	AC-18
DS-4.1		9.1, 13.1	AC-18
DS-4.2		9.1, 13.1	SI-4
DS-5.0	I/O Device Security	10.7.1	SC-7
DS-5.1			AC-19, MP-2
DS-6.0	System Security	12.2	SI-3
DS-6.1		12.2	SI-3
DS-6.2		12.2	SI-3
DS-6.3		12.2	SI-3
DS-6.4		12.5, 12.6	SI-2, RA-5
DS-6.5		9.4	AC-5, SC-2
DS-6.6		11.2	PE-3
DS-6.7		6.2, 10.1, 11.1	MA-4, PE-5
DS-6.8		8.1, 12.5	CM-11 SI-7
DS-6.9		12.1, 12.5	CM-10, SI-7
DS-6.10		12.6	AC-3, AC-6, CM-7
DS-6.11		8.1	CM-8
DS-6.12		8.1, 14.1, 14.2	
DS-7.0	Account Management	9	AC-2
DS-7.1		9.1	AC-2
DS-7.2		9.2, 9.4	AC-2, AC-6, IA-4
DS-7.3		8.1, 9.2, 9.4	AC-2, AC-6, IA-4
DS-7.4		12.4, 18.2	AC-2, AC-6, IA-4
DS-7.5		12.1, 12.4	AU-3, AU-6
DS-7.6		9.2, 9.4	AU-2, AU-12
DS-7.7		9.2, 9.4	PS-4, PS-5
DS-7.8		9.2, 9.4	AC-2, PE-2
DS-8.0	Authentication	9.1	IA-2, IA-4
DS-8.1		9	AC-7, IA-5, IA-2
DS-8.2		9.4, 10.1	AC-17
DS-8.3		9.2, 9.4	AC-11
DS-8.4		9.4	AC-1
DS-9.0	Logging and Monitoring	12.4	SI-4, AU-2, AU-3
DS-9.1		12.4	AU-1, AU-6

No.	Security Topic	ISO 27002 -2013 Reference	NIST 800-53 Rev. 4 Reference
DS-9.2		12.4	AU-1, AU-6
DS-9.3		12.4	AU-1, AU-2, AU-6
DS-9.4		10.1	AU-2, AU-3
DS-9.5		12.4	AU-3, AU-8
DS-9.6		12.4	AU-9, AU-11
DS-9.7		12.4	AU-6
DS-10.0	Mobile Security	6.2, 11.2	SC, AC, IA-2
DS-10.1		6.2, 11.2	SC, AC
DS-10.2		6.2, 11.2	SC, AC
DS-10.3		6.2, 11.2	SC, AC
DS-10.4		6.2, 11.2	SC, AC
DS-10.5		6.2, 11.2	SC, AC
DS-10.6		6.2, 11.2	SC, AC
DS-10.7		6.2, 11.2	SC, AC
DS-10.8		6.2, 11.2	SC, AC
DS-10.9		6.2, 11.2	SC, AC
DS-11.0	Security Techniques	8.2, 10.1	
DS-11.1		8.2, 10.1	IA-5, SC-13
DS-11.2		8.2, 10.1	SC-8, SC-12
DS-11.3		8.2, 10.1	SC-12
DS-11.4			
DS-11.5			
DS-11.6		10.1	
DS-11.7		10.1	

No.	Security Topic	ISO 27002 -2013 Reference	NIST 800-53 Rev. 4 Reference
DS-12.0	Content Tracking		
DS-12.1			
DS-12.2			
DS-12.3			
DS-13.0	Transfer Systems	10.1, 13.2	IA-5, SC-13
DS-13.1		10.1, 13.2	
DS-14.0	Transfer Device Methodology	13.1	
DS-14.1		13.1	AC-4, SC-7
DS-14.2		13.1	AC-4, AC-20, SC-7
DS-14.3		13.2	MP-6
DS-14.4		12.4, 13.2	
DS-15.0	Client Portal	13.1	AC-6
DS-15.1		9.2, 9.4	IA-5
DS-15.2		9.2, 9.4	AC-2, AC-3, AC-6
DS-15.3		12.6, 13.1	AC-4, AC-20
DS-15.4		9.2, 9.4, 10.1	
DS-15.5		10.1	SC-8, SC-13
DS-15.6		9.4	AC-4
DS-15.7		9.4	AC-2
DS-15.8		12.6	SI-7
DS-15.9		12.6	
DS-15.10			
DS-15.11		13.2	AC-4
DS-15.12		12.1	

APPENDIX D — 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
   - Note: include everything (acceptable use, etc.)
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)
   - Records retention
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 E — 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://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

National Institute of Standards and Technology Special Publication IR 7298. *Glossary of Key Information Security Terms,* April 2006. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.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://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

National Industrial Security Program - Operating Manual (DoD 5220.22-M), February 2006 http://dtic.mil/whs/directives/corres/pdf/522022m.pdf

The Center for Internet Security – Security Benchmarks http://benchmarks.cisecurity.org/

National Security Agency - Security Configuration Guides https://www.nsa.gov/ia/mitigation_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

End of Document