AWS alignment with Motion Picture of America Association (MPAA) Content Security Model

The Motion Picture of America Association (MPAA) has established a set of best practices for securely storing, processing and delivering protected media and content. For additional information on MPAA content security best practices refer to: http://www.fightfilmtheft.org/best-practice.html.

The table below was created by AWS to highlight the delta between the MPAA best practices published in 2013 and the MPAA best practices published in 2015.
- For any new control added to the 2015 MPAA best practices, see any rows highlighted in "green."
- For any control set which had a slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "blue."
- For any control set which was removed from the 2015 MPAA best practices, these controls were highlighted in "grey."
- Any control set which is not highlighted the requirements behind the controls were fundamentally unchanged.

MPAA Best Practices 2015			MPAA Best Practices 2013			AWS comments on the differences between 2015 and 2013 version
Security Topic	No.	Best Practice	Security Topic	No.	Best Practice	
Executive Security Awareness/ Oversight	MS-1.0	Establish an information security management system that implements a control framework for information security which is approved by the business owner(s) /senior management.	Executive Security Awareness / Oversight	MS.S-1.0	Establish an information security management system that implements a control framework (e.g., ISO 27001) for information security which is approved by executive management/owner(s)	The difference with the 2015 standard is the requirement for policies and processes to be reviewed at least annually vs. periodically
	MS-1.1	Review information security management policies and processes at least annually.		MS-1.1	Train and engage executive management/owner(s) on the business' responsibilities to protect content	
	MS-1.2	Train and engage executive management/owner(s) on the business' responsibilities to protect content at least annually.		MS-1.0	Ensure executive management/owner(s) oversight of the Information Security function by requiring periodic review of the information security program and risk assessment results	
	MS-1.3	Create an information security management group to establish and review information security management policies.				
Risk Management	MS-2.0	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.	Risk Management	MS-2.1	Identify high-security content based on client instruction	The difference with the 2015 standard is the requirement for a formalized risk assessment process vs. based on client instruction.
	MS-2.1	Conduct an internal risk assessment annually and upon key workflow changes—based on, at a minimum, the MPAA Best Practice Common Guidelines and the applicable Supplemental Guidelines—and document and act upon identified risks.		MS-2.2	Conduct an internal risk assessment annually and upon key workflow changes—based on, at a minimum, the MPAA Best Practice Common Guidelines and the applicable Supplemental Guidelines—and document and act upon identified risks	
Security Organization	MS-3.0	Identify security key point(s) of contact and formally define roles and responsibilities for content and asset protection.	Security Organization	MS-3.0	Identify security key point(s) of contact and formally define roles and responsibilities for content and asset protection	With the 2015 standard, the requirement for establishing a security team was removed.
				MS.S-3.0	Establish a security team that is responsible for proactively monitoring information systems and physical security to identify and respond to any suspicious activity	
Policies and Procedures	MS-4.0	Establish policies and procedures regarding asset and content security; policies should address the following topics, at a minimum: • Acceptable use (e.g., social networking, Internet, phone, personal devices, mobile devices, etc.) • Asset and content classification and handling policies • Business continuity (backup, retention and restoration) • 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)	Policies and Procedures	MS-4.0	Establish policies and procedures regarding asset and content security; policies should address the following topics, at a minimum: • Human resources policies • Acceptable use (e.g., social networking, Internet, phone, etc.) • Asset classification • Asset handling policies • Digital recording devices (e.g., smart phones, digital cameras, camcorders) • Exception policy (e.g., process to document policy deviations) • Password controls (e.g., password minimum length, screensavers) • Prohibition of client asset removal from the facility • System change management • Whistleblower policy • Sanction policy (e.g., disciplinary policy)	With the 2015 standard, the requirement for a human resource policy and client asset removal - were removed. The requirement for policies around business continuity, confidentiality, incident response, mobile device, network: internet and wireless, security policy, visitor policy, and disciplinary - were added.
	MS-4.1	Review and update security policies and procedures at least annually.		MS.S-4.0	Provide in-depth training specific to the content handled by the facility	
	MS-4.2	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.		MS-4.1	Review and update security policies and procedures at least annually	
	MS-4.3	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 • Security incident reporting and escalation • Disciplinary policy • Encryption and key management for all individuals who handle encrypted content • Asset disposal and destruction processes		MS.S-4.1	Provide training on the applications and processes surrounding encryption and key management for all individuals who handle encrypted content	
				MS-4.2	Require a sign-off from all company personnel (e.g., employees, temporary workers, interns) and third party workers (e.g., contractors, freelancers, temp agencies) for all policies, procedures, and/or client requirements and any updates	
				MS-4.3	Develop and regularly update a security awareness program and train company personnel and third party workers upon hire and annually thereafter on the security policies and procedures, addressing the following areas at a minimum: • IT security policies and procedures • Content/asset security and handling • Security incident reporting and escalation • Disciplinary measures	
Incident Response	MS-5.0	Establish a formal incident response plan that describes actions to be taken when a security incident is detected and reported.	Incident Response	MS-5.0	Establish a formal incident response plan that describes actions to be taken when a security incident is detected and reported	The control requirements behind the control set did not change between 2015 and 2013.
	MS-5.1	Identify the security incident response team who will be responsible for detecting, analyzing, and remediating security incidents.		MS-5.1	Identify the security incident response team who will be responsible for detecting, analyzing, and remediating security incidents	
	MS-5.2	Establish a security incident reporting process for individuals to report detected incidents to the security incident response team.		MS-5.2	Establish a security incident reporting process for individuals to report detected incidents to the security incident response team	
	MS-5.3	Communicate 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.		MS-5.3	Communicate 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	
Business Continuity & Disaster Recovery	MS-6.0	Establish a formal plan that describes actions to be taken to ensure business continuity.				2015 MPAA added this control set.
	MS-6.1	Identify the business continuity team who will be responsible for detecting, analyzing and remediating continuity incidents.				
Change Control & Configuration Management	MS-7.0	Establish policies and procedures to ensure new data, applications, network, and systems components have been pre-approved by business leadership.				2015 MPAA added this control set.
Workflow	MS-8.0	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	Workflow	MS-6.0	Document a workflow that includes the tracking of content and authorization checkpoints throughout each process; include the following processes for both physical and digital content: • Delivery • Ingest • Movement • Storage • Return to originator • Removal from the site • Destruction	The control requirements behind the control set did not change between 2015 and 2013.
	MS-8.1	Update the workflow when there are changes to the process, and review the workflow process at least annually to identify changes.		MS-6.1	Identify, implement, and assess the effectiveness of key controls to prevent, detect, and correct risks related to the content workflow	
Segregation of Duties	MS-9.0	Segregate duties within the content workflow. Implement and document compensating controls where segregation is not practical.	Segregation of Duties	MS-7.0	Segregate duties within the content workflow, and implement and document compensating controls where segregation is not practical	The control requirements behind the control set did not change between 2015 and 2013.
Background Checks	MS-10.0	Perform background screening checks on all company personnel and third party workers.	Background Checks	MS-8.0	Perform background screening checks on all company personnel and third party workers	The control requirements behind the control set did not change between 2015 and 2013.
Confidentiality Agreements	MS-11.0	Require all company personnel to sign a confidentiality agreement (e.g., non-disclosure) upon hire and annually thereafter, that includes requirements for handling and protecting content.	Confidentiality Agreements	MS-9.0	Require all company personnel and third party workers to sign a confidentiality agreement (e.g., non-disclosure) upon hire and annually thereafter, that includes requirements for handling and protecting content	The control requirements behind the control set did not change between 2015 and 2013.
	MS-11.1	Require all company personnel to return all content and client information in their possession upon termination of their employment or contract.		MS-9.1	Require all company personnel and third party workers to return all content and client information in their possession upon termination of their employment or contract	
	MS-12.0	Require all third party workers (e.g., freelancers) who handle content to sign confidentiality agreements (e.g., non-disclosure) upon engagement.		MS-10.0	Require all third party workers who handle content to sign confidentiality agreements (e.g., non-disclosure) upon engagement	The 2015 MPAA has generalized the use of 3rd parties, the prior MPAA mapping required 3rd parties be "Customs-Trade Partnership Against Terrorism" (CTPAT) certified. Additionally, the requirement for training

The Motion Picture of America Association (MPAA) has established a set of best practices for securely storing, processing and delivering protected media and content. For additional information on MPAA content security best practices refer to: http://www.fightfilmtheft.org/best-practice.html.

The table below was created by AWS to highlight the delta between the MPAA best practices published in 2013 and the MPAA best practices published in 2015.
- For any new control added to the 2015 MPAA best practices, see any rows highlighted in "green."
- For any control set which had a slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "blue."
- For any control set which was removed from the 2015 MPAA best practices, these controls were highlighted in "grey."
- Any control set which is not highlighted the requirements behind the controls were fundamentally unchanged.

MPAA Best Practices 2015			MPAA Best Practices 2013			AWS comments on the differences between 2015 and 2013 version
Security Topic	**No.**	**Best Practice**	**Security Topic**	**No.**	**Best Practice**	
Third Party Use and Screening	MS-12.1	Require all third party workers to return all content and client information in their possession upon termination of their contract.	Third Party Use and Screening	MS.S-10.0	Communicate to clients the use of third-party storage providers for physical assets	and annual evaluation was removed.
	MS-12.2	Include security requirements in third party contracts.		MS-10.1	Include security requirements in third party contracts	
	MS-12.3	Implement a process to reclaim content when terminating relationships.		MS.S-10.1	Require international (to/from U.S.) transportation companies to be "Customs-Trade Partnership Against Terrorism" (CTPAT) certified	
	MS-12.4	Require third party workers to be bonded and insured where appropriate (e.g., courier service).		MS-10.2	Implement a process to reclaim assets and remind third party workers of confidentiality agreements and contractual security requirements when terminating relationships	
	MS-12.5	Restrict third party access to content/production areas unless required for their job function.		MS.S-10.2	Re-assess transportation and packaging vendors annually and when the vendor changes its location and/or provides additional services	
	MS-12.6	Notify clients if subcontractors are used to handle content or work is offloaded to another company.		MS-10.3	Require third party workers to be bonded and insured where appropriate (e.g., courier service)	
				MS.S-10.3	Review access to third-party content delivery systems and websites annually	
				MS-10.4	Restrict third party access to content/production areas unless required for their job function	
				MS.S-10.4	Incorporate security due diligence activities (e.g., security assessment, self-assessment questionnaire) as part of a selection and hiring process for third party workers who handle sensitive content	
				MS-10.5	Require third party companies to notify clients if they are on-boarding additional third party companies to handle content	
Entry/Exit Points	PS-1.0	Secure all entry/exit points of the facility at all times, including loading dock doors and windows.	Entry/Exit Points	PS-1.0	Lock all entry/exit points at all times if the facility does not have a segregated access-controlled area beyond reception	The MPAA 2015 has removed the requirements which specify the needs of a security guard, including the security patrols and investigation of incidents discovered by a security guard.
	PS-1.1	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).		PS.S-1.0	Post security guards at all non-emergency entry/exit points	
	PS-1.2	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-1.1	Control access to areas where content is handled by segregating the content area from other facility areas (e.g., administrative offices)	
				PS.S-1.1	Lock and install alarms on all loading dock doors, and monitor loading dock doors while in use	
				PS.S-1.2	Segregate the truck driver's entrance to prevent truck drivers from entering other areas of the facility	
				PS.S-1.3	Implement a daily security patrol process with a randomized schedule and document the patrol results in a log	
				PS.S-1.4	Document, investigate, and resolve all incidents detected during security guard shifts	
Visitor Entry/Exit	PS-2.0	Maintain a detailed visitors' log and include the following: • Name • Company • Time in/time out • Person/people visited • Signature of visitor • Badge number assigned	Visitor Entry/Exit	PS-2.0	Maintain a detailed visitors' log which includes the following: • Name • Company • Time in/time out • Person/people visited • Signature of visitor • Badge number assigned	The control requirements behind the control set did not change between 2015 and 2013.
	PS-2.1	Assign an identification badge or sticker which must be visible at all times, to each visitor and collect badges upon exit.		PS-2.1	Assign an identification badge or sticker, which must be visible at all times, to each visitor and collect badges upon exit	
	PS-2.2	Do not provide visitors with key card access to content/production areas.		PS-2.2	Do not provide visitors with electronic access to content/production areas	
	PS-2.3	Require visitors to be escorted by authorized employees while on-site, or in content/production areas.		PS-2.3	Require visitors to be escorted by authorized employees while on-site, or in content/production areas at a minimum	
Identification	PS-3.0	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.	Identification	PS-3.0	Provide company personnel and long-term third party workers (e.g., janitorial) with photo identification that is validated and required to be visible at all times	The control requirements behind the control set did not change between 2015 and 2013.
Perimeter Security	PS-4.0	Implement perimeter security controls that address risks that the facility may be exposed to as identified by the organization's risk assessment.	Perimeter Security	PS-4.0	Implement perimeter security controls that address risks that the facility may be exposed to as identified by the organization's risk assessment	2015 MPAA has slight change in the perimeter security requirements, instead of having security guard stationed at the entrance/exits - the standard is asking for a process w/randomized schedules.
	PS-4.1	Place security guards at perimeter entrances and non- emergency entry/exit points.		PS.S-4.0	Install additional perimeter safeguards (e.g., fences, vehicle barricades) to decrease the risk of unauthorized access onto the premises	
	PS-4.2	Implement a daily security patrol process with a randomized schedule and document the patrol results in a log.		PS.S-4.1	Lock perimeter gates at all times and dedicate an on-site employee to handle remote unlocking capabilities	
	PS-4.3	Lock perimeter gates at all times.		PS.S-4.2	Station a security guard at perimeter entrances and implement a process (e.g., electronic gate arm, parking permits) to allow vehicles into the facility campus	
Alarms	PS-5.0	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.).	Alarms	PS-5.0	Install a centralized, audible alarm system that covers all entry/exit points (including emergency exits), loading docks, fire escapes, and restricted areas (e.g., vault, server/machine room)	2015 MPAA has added the addition of fire safety measures in the event of a power outage. Additionally, the alarms should be tested quarterly vs. semi-annually.
	PS-5.1	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.).		PS-5.1	Configure alarms to provide escalation notifications directly to the personnel in charge of security and/or be monitored by a central security group or third party	
	PS-5.2	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).		PS-5.2	Assign unique arm and disarm codes to each person that requires access to the alarm system and restrict access to all other personnel	
	PS-5.3	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.).		PS-5.3	Review the list of users who can arm and disarm alarm systems annually	
	PS-5.4	Assign unique arm and disarm codes to each person that requires access to the alarm system and restrict access to all other personnel.		PS-5.4	Test the alarm system every 6 months	
	PS-5.5	Review the list of users who can arm and disarm alarm systems quarterly, or upon change of personnel.		PS-5.5	Install and effectively position motion detectors in restricted areas (e.g., vault, server/machine room) and configure them to alert the appropriate security personnel and/or third-party	
	PS-5.6	Test the alarm system quarterly.		PS-5.6	Install door prop alarms for content/production areas to notify when sensitive entry/exit points are open for longer than a pre-determined period of time (e.g., 60 seconds)	
	PS-5.7	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.				
Authorization	PS-6.0	Document and implement a process to manage facility access and keep records of any changes to access rights.	Authorization	PS-6.0	Document and implement a process to manage facility access and keep records of any changes to access rights	2015 MPAA removed the requirement to review restricted access on a monthly basis.
	PS-6.1	Restrict access to production systems to authorized personnel only.		PS.S-6.0	Review access to restricted areas (e.g., vault, safe) on a monthly basis and when the roles or employment status of any company personnel and/or third party workers change	
	PS-6.2	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.		PS-6.1	Restrict access to production systems to authorized personnel only	
				PS-6.2	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	
Electronic Access Control	PS-7.0	Implement electronic access throughout the facility to cover all entry/exit points and all areas where content is stored, transmitted, or processed.	Electronic Access	PS-7.0	Implement electronic access throughout the facility to cover all entry/exit points and all areas where content is stored, transmitted, or processed	2015 MPAA removed the requirement to implement separate rooms for replication and for mastering.
	PS-7.1	Restrict electronic access system administration to appropriate personnel.		PS.S-7.0	Establish separate rooms for replication and for mastering	
	PS-7.2	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.		PS-7.1	Restrict electronic access system administration to appropriate personnel	
	PS-7.3	Disable lost electronic access devices (e.g., keycards, key fobs) in the system before issuing a new electronic access device.		PS-7.2	Store blank card stock in a locked cabinet and ensure keycards remain disabled prior to being assigned to personnel	

The Motion Picture of America Association (MPAA) has established a set of best practices for securely storing, processing and delivering protected media and content. For additional information on MPAA content security best practices refer to: http://www.fightfilmtheft.org/best-practice.html.

The table below was created by AWS to highlight the delta between the MPAA best practices published in 2013 and the MPAA best practices published in 2015.
- For any new control added to the 2015 MPAA best practices, see any rows highlighted in "green."
- For any control set which had a slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "blue."
- For any control set which was removed from the 2015 MPAA best practices, these controls were highlighted in "grey."
- Any control set which is not highlighted the requirements behind the controls were fundamentally unchanged.

MPAA Best Practices 2015			MPAA Best Practices 2013			AWS comments on the differences between 2015 and 2013 version
Security Topic	No.	Best Practice	Security Topic	No.	Best Practice	
	PS-7.4	Issue third party access electronic access devices with a set expiration date (e.g. 90 days) based on an approved timeframe.		PS-7.3 PS-7.4	Disable lost keycards in the system before issuing a new keycard Issue third party access cards with a set expiration date (e.g. 90 days) based on an approved timeframe	
Keys	PS-8.0 PS-8.1 PS-8.2 PS-8.3 PS-8.4 PS-8.5	Limit the distribution of master keys and / or keys to restricted areas to authorized personnel only (e.g., owner, facilities management). Implement a check-in/check-out process to track and monitor the distribution of master keys and / or keys to restricted areas. Use keys that can only be copied by a specific locksmith for exterior entry/exit points. Inventory master keys and keys to restricted areas, including facility entry/exit points, quarterly. Obtain all keys from terminated employees/third-parties or those who no longer need the access. Implement electronic access control or rekey entire facility when master or sub-master keys are lost or missing.	Keys	PS-8.0 PS-8.1 PS-8.2 PS-8.3	Limit the distribution of master keys to authorized personnel only (e.g., owner, facilities management) Implement a check-in/check-out process to track and monitor the distribution of master keys Use keys that can only be copied by a specific locksmith for exterior entry/exit points Inventory master keys and keys to restricted areas, including facility entry/exit points, quarterly	2015 MPAA added additional controls on retrieving keys from terminated/third party employees. Additionally, the process of implementing electronic access controls and rekeying the entire facility when a master key is lost.
Cameras	PS-9.0 PS-9.1 PS-9.2 PS-9.3 PS-9.4	Install a CCTV system that records all facility entry/exit points and restricted areas (e.g. server/machine room, etc.). Review camera positioning and recordings to ensure adequate coverage, function, image quality, lighting conditions and frame rate of surveillance footage at least daily. Restrict physical and logical access to the CCTV console and to CCTV equipment (e.g., DVRs) to personnel responsible for administering/monitoring the system. Ensure that camera footage includes an accurate date and time-stamp and retain CCTV surveillance footage and electronic access logs for at least 90 days, or the maximum time allowed by law, in a secure location. Designate an employee or group of employees to monitor surveillance footage during operating hours and immediately investigate detected security incidents.	Cameras	PS-9.0 PS.S-9.0 PS-9.1 PS.S-9.1 PS-9.2 PS-9.3	Install a CCTV system that records all facility entry/exit points and restricted areas Review camera positioning, image quality, frame rate and retention daily Review camera positioning, image quality, lighting conditions, frame rate, and adequate retention of surveillance footage at least weekly Designate an employee or group of employees to monitor surveillance footage during operating hours and immediately investigate detected security incidents Restrict physical and logical access to the CCTV console and to CCTV equipment (e.g., DVRs) to personnel responsible for administering/monitoring the system Ensure that camera footage includes an accurate date and time-stamp	The control requirements behind the control set did not change between 2015 and 2013.
Logging and Monitoring	PS-10.0 PS-10.1 PS-10.2 PS-10.3	Log and review electronic access to restricted areas for suspicious events, at least weekly. 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 Investigate suspicious electronic access activities that are detected. Maintain an ongoing log of all confirmed electronic access incidents and include documentation of any follow-up activities that were taken.	Logging and Monitoring	PS-10.0 PS.S-10.0 PS-10.1 PS-10.2 PS-10.3	Log and review electronic access to restricted areas for suspicious events Perform a weekly review of electronic access logs for the following areas, if applicable: • Masters/stampers vault • Pre-mastering • Server/machine room • Scrap room • High-security cages Investigate suspicious electronic access activities that are detected Maintain an ongoing log of all confirmed electronic access incidents and include documentation of any follow-up activities that were taken Retain CCTV surveillance footage and electronic access logs for at least 90 days, or the maximum time allowed by law, in a secure location	2015 MPAA removed the control regarding the retention of CCTV surveillance footage.
Searches	PS-11.0 PS-11.1 PS-11.2 PS-11.3 PS-11.4 PS-11.5 PS-11.6 PS-11.7 PS-11.8 PS-11.9	Establish a policy, as permitted by local laws, that allows security to randomly search persons, bags, packages, and personal items for client content. 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 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. Enforce the use of transparent plastic bags and food containers for any food brought into production areas. Implement a dress code policy that prohibits the use of oversized clothing (e.g., baggy pants, oversized hooded sweatshirts). Use numbered tamper-evident stickers/holograms to identify authorized devices that can be taken in and out of the facility. Implement a process to test the exit search procedure. Perform a random vehicle search process when exiting the facility parking lot. Segregate replication lines that process highly sensitive content and perform searches upon exiting segregated areas. Implement additional controls to monitor security guards activity.	Searches	PS-11.0 PS.S-11.0 PS.S-11.1 PS.S-11.2 PS.S-11.3 PS.S-11.4 PS.S-11.5 PS.S-11.6 PS.S-11.7 PS.S-11.8	Inform company personnel and third party workers upon hire that bags and packages are subject to random searches and include a provision addressing searches in the facility policies 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 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 Enforce the use of transparent plastic bags and food containers for any food brought into production areas Implement a dress code policy that prohibits the use of oversized clothing (e.g., baggy pants, oversized hooded sweatshirts) Use numbered, tamper-evident stickers/holograms to identify authorized devices that can be taken in and out of the facility Implement a process to test the exit search procedure Perform a random vehicle search process when exiting the facility parking lot Segregate replication lines that process highly sensitive content and perform searches upon exiting segregated areas Implement additional controls to monitor security guard activity	The control requirements behind the control set did not change between 2015 and 2013.
Inventory Tracking	PS-12.0 PS-12.1 PS-12.2 PS-12.3 PS-12.4 PS-12.5 PS-12.6	Implement a content asset management system to provide detailed tracking of physical assets (i.e., received from client created at the facility). 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. Retain asset movement transaction logs for at least one year. Review logs from content asset management system at least weekly and investigate anomalies. Use studio film title aliases when applicable on physical assets and in asset tracking systems. Implement and review a daily aging report to identify highly sensitive assets that are checked out from the vault and not checked back in. Lock up and log assets that are delayed or returned if shipments could not be delivered on time.	Inventory Tracking	PS-12.0 PS.S-12.0 PS-12.1 PS.S-12.1 PS-12.2 PS-12.3 PS-12.4	Implement a content asset management system to provide detailed tracking of physical assets (i.e., client and newly created) Use automated notification for assets that have been out of the vault for extended periods of time Barcode client assets and created media (e.g., tapes, hard drives) upon receipt and store assets in the vault when not in use Lock up and log assets that are delayed or returned if shipments could not be delivered on time Retain asset movement transaction logs for at least 90 days Review logs from content asset management system and investigate anomalies Use studio AKAs ("aliases") when applicable in asset tracking systems and on any physical assets	2015 MPAA removed the requirement to use automated notification for assets that have been out of the vault for extended periods of time. Additionally, added the requirement to implement and review a daily aging report to identify highly sensitive assets that are checked out from the vault and not checked back in.
Inventory Counts	PS-13.0 PS-13.1	Perform a quarterly inventory count of each client's asset(s), reconcile against asset management records, and immediately communicate variances to clients. Segregate duties between the vault staff and individuals who are responsible for performing inventory counts.	Inventory Counts	PS-13.0 PS.S-13.0 PS-13.1 PS.S-13.1 PS-13.2	Perform a quarterly inventory count of each client's pre-release project(s), reconcile against asset management records, and immediately communicate variances to clients Perform a weekly inventory count of each client's pre-release project(s), reconcile against asset management records, and immediately communicate variances to clients Segregate duties between the vault staff and individuals who are responsible for performing inventory counts Monitor film elements (e.g., negatives, unprocessed film) constantly throughout the workflow process Implement and review a daily aging report to identify highly sensitive assets that are checked out from the vault and not checked back in	2015 MPAA removed the requirement to perform a weekly inventory count of client's pre-release projects and the requirement to monitor film elements throughout the workflow process. Additionally, the requirement to implement and review a daily aging report.
Blank Media/ Raw Stock Tracking	PS-14.0 PS-14.1 PS-14.2	Tag (e.g., barcode, assign unique identifier) blank stock/raw stock per unit when received. Establish a process to track consumption of raw materials (e.g., polycarbonate) monthly. Store blank media/raw stock in a secured location.	Blank Media/ Raw Stock Tracking	PS-14.0 PS.S-14.0 PS-14.1	Tag (e.g., barcode, assign unique identifier) blank stock/raw stock per unit when received Establish a process to track consumption of raw materials (e.g., polycarbonate) monthly Store blank media/raw stock in a secured location	The control requirements behind the control set did not change between 2015 and 2013.
Client Assets	PS-15.0 PS-15.1 PS-15.2 PS-15.3	Restrict access to finished client assets to personnel responsible for tracking and managing assets. Store client assets in a restricted and secure area (e.g., vault, safe, or other secure storage location). Require two company personnel with separate access cards to unlock highly sensitive areas (e.g., safe, high-security cage) after-hours. Use a locked fireproof safe to store undelivered packages that are kept at the facility overnight.	Client Assets	PS-15.0 PS.S-15.0 PS-15.1 PS.S-15.1	Restrict access to finished client assets to personnel responsible for tracking and managing assets Require two company personnel with separate access cards to unlock highly sensitive areas (e.g., safe, high-security cage) after-hours Store client assets in a restricted and secure area (e.g., vault, safe) Use an access-controlled cage for the staging area and monitor the area with surveillance cameras	2015 MPAA removes the requirement to use an access-controlled cage for the staging area and monitor the area with surveillance cameras

The Motion Picture of America Association (MPAA) has established a set of best practices for securely storing, processing and delivering protected media and content. For additional information on MPAA content security best practices refer to: http://www.fightfilmtheft.org/best-practice.html.

The table below was created by AWS to highlight the delta between the MPAA best practices published in 2013 and the MPAA best practices published in 2015.
- For any new control added to the 2015 MPAA best practices, see any rows highlighted in "green."
- For any control set which had a slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "blue."
- For any control set which was removed from the 2015 MPAA best practices, these controls were highlighted in "grey."
- Any control set which is not highlighted the requirements behind the controls were fundamentally unchanged.

MPAA Best Practices 2015			MPAA Best Practices 2013			AWS comments on the differences between 2015 and 2013 version
Security Topic	**No.**	**Best Practice**	**Security Topic**	**No.**	**Best Practice**	
	PS-15.4	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.		PS.S-15.2	Use a locked fireproof safe to store undelivered packages that are kept at the facility overnight	
				PS.S-15.3	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	
Disposals	PS-16.0	Require that rejected, damaged, and obsolete stock containing client assets are erased, degaussed, shredded, or physically destroyed before disposal.	Disposals	PS-16.0	Require that rejected, damaged, and obsolete stock are erased, degaussed, shredded, or physically destroyed before disposal (e.g., DVD shredding, hard drive destruction) and update asset management records to reflect destruction	2015 MPAA does not specifically call out the requirements needed for third parties. Nor the requirement to scratch discs before placing them in the scrap bin.
	PS-16.1	Store elements targeted for recycling/destruction in a secure location/container to prevent the copying and reuse of assets prior to disposal.		PS.S-16.0	Implement a process that requires security personnel to monitor and record the scrapping process if scrap is destroyed	
	PS-16.2	Maintain a log of asset disposal for at least 12 months.		PS-16.1	Store elements targeted for recycling/destruction in a secure location/container to prevent the copying and reuse of assets prior to disposal	
	PS-16.3	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.		PS.S-16.1	Conduct periodic security training for all company personnel and third party workers to educate on asset disposal and destruction processes (e.g., placing assets into designated containers)	
	PS-16.4	Use automation to transfer rejected discs from replication machines directly into scrap bins (no machine operator handling).		PS-16.2	Maintain a log of asset disposal for at least 12 months	
				PS.S-16.2	Scratch discs before placing them into the scrap bin	
				PS-16.3	Require third-party companies who handle destruction of content to provide a certificate of destruction for each completed job	
				PS.S-16.3	Use automation to transfer rejected discs from replication machines directly into scrap bins (no machine operator handling)	
				PS.S-16.4	Prohibit the use of third party companies for the destruction of DCDM drives or pre-released content	
Shipping	PS-17.0	Require the facility to generate a valid work/shipping order to authorize client asset shipments out of the facility.	Shipping	PS-17.0	Require the facility to file a valid work/shipping order to authorize asset shipments out of the facility	2015 MPAA requires assets in transit are tracked and logged with shipping details.
	PS-17.1	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		PS.S-17.0	Document and retain a separate log for truck driver information	
	PS-17.2	Secure client assets that are waiting to be picked up.		PS-17.1	Track and log asset shipping details; at a minimum, include the following: • Time of shipment • Sender name and signature • Recipient name • Address of destination • Tracking number from courier • Reference to the corresponding work order	
	PS-17.3	Validate client assets leaving the facility against a valid work/shipping order.		PS.S-17.1	Require personnel picking up package(s) to verify the count the shipping document and obtain a signature from the shipping point	
	PS-17.4	Prohibit couriers and delivery personnel from entering content/production areas of the facility.		PS-17.2	Validate assets leaving the facility against a valid work/shipping order	
	PS-17.5	Document and retain a separate log for truck driver information.		PS.S-17.2	Observe and monitor the packing and sealing of trailers when shipping occurs on-site	
	PS-17.6	Observe and monitor the on-site packing and sealing of trailers prior to shipping.		PS-17.3	Secure assets that are waiting to be picked up	
	PS-17.7	Record, monitor and review travel times, routes, and delivery times for shipments between facilities.		PS.S-17.3	Implement a formal process to record, monitor, and review travel times, routes, and delivery times for shipments between facilities	
	PS-17.8	Prohibit the transfer of film elements other than for client studio approved purposes.		PS-17.4	Prohibit couriers and delivery personnel from entering content/production areas of the facility	
	PS-17.9	Ship prints for pre-theatrical screenings in segments (e.g., odd versus even reels).		PS.S-17.4	Do not allow film elements to leave the facility other than through shipping, except with a signed authorization pass	
				PS.S-17.5	Ship prints for pre-theatrical screenings in segments (e.g., odd versus even reels)	
Receiving	PS-18.0	Inspect delivered client assets upon receipt and compare to shipping documents (e.g., packing slip, manifest log).	Receiving	PS-18.0	Inspect delivered content upon receipt and compare to shipping documents (e.g., packing slip, manifest log)	The control requirements behind the control set did not change between 2015 and 2013.
	PS-18.1	Maintain a receiving log to be filled out by designated personnel upon receipt of deliveries.		PS-18.1	Maintain a receiving log to be filled out by designated personnel upon receipt of deliveries	
	PS-18.2	Perform the following actions immediately: • Tag (e.g., barcode, assign unique identifier) received assets • Input the asset into the asset management system • Move the asset to the restricted area (e.g., vault, safe)		PS-18.2	Perform the following actions immediately: • Tag (e.g., barcode, assign unique identifier) received assets, • Input the asset into the asset management system • Move the asset to the restricted area (e.g., vault, safe)	
	PS-18.3	Implement a secure method for receiving overnight deliveries.		PS-18.3	Implement a secure method (e.g., secure drop box) for receiving overnight deliveries	
Labeling	PS-19.0	Prohibit the use of title information, including AKAs ("aliases"), on the outside of packages unless instructed otherwise by client.	Labeling	PS-19.0	Prohibit the use of title information, including AKAs ("aliases"), on the outside of packages	The control requirements behind the control set did not change between 2015 and 2013.
Packaging	PS-20.0	Ship all client assets in closed/sealed containers, and use locked containers depending on asset value, or if instructed by the client.	Packaging	PS-20.0	Ship all assets in closed/sealed containers, and use locked containers depending on asset value	The control requirements behind the control set did not change between 2015 and 2013.
	PS-20.1	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)		PS.S-20.0	Apply shrink wrapping to all shipments, and inspect packaging before final shipment to ensure that it is adequately wrapped	
	PS-20.2	Apply shrink wrapping to all shipments, and inspect packaging before final shipment to ensure that it is adequately wrapped.		PS-20.1	Implement at least one of the following controls: • Tamper-evident tape • Tamper-evident packaging • Tamper-evident seals in the form of holograms • Secure containers (e.g., Pelican case with a combination lock)	
Transport Vehicles	PS-21.0	Lock automobiles and trucks at all times, and do not place packages in clear view.	Transport Vehicles	PS-21.0	Lock automobiles and trucks at all times, and do not place packages in visible auto/truck areas	The control requirements behind the control set did not change between 2015 and 2013.
	PS-21.1	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		PS.S-21.0	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	
	PS-21.2	Apply numbered seals on cargo doors for shipments of highly sensitive titles.		PS.S-21.1	Apply numbered seals on cargo doors for shipments of highly sensitive titles	
	PS-21.3	Require security escorts to be used when delivering highly sensitive content to high-risk areas.		PS.S-21.2	Require security escorts be used for delivery of highly sensitive content in high-risk areas	
Firewall/WAN/ Perimeter Security	DS-1.0	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.	WAN	DS-1.0	Segment WAN(s) by using stateful inspection firewalls with Access Control Lists that prevent unauthorized access to any internal network	2015 MPAA added the requirements to perform quarterly vuln scans of external IP ranges, secure any point to point connections by using dedicated, private connections and by using encryption. Additionally the requirement to implement baseline security requirements for WAN network infrastructure devices and services.
	DS-1.1	Implement a process to review firewall Access Control Lists (ACLs) to confirm configuration settings are appropriate and required by the business every 6 months.		DS-1.1	Develop a process to review firewall Access Control Lists (ACLs) to confirm configuration settings are appropriate and required by the business every 6 months	
	DS-1.2	Deny all protocols by default and enable only specific permitted secure protocols to access the WAN and firewall.		DS-1.2	Deny all protocols by default and enable only specific permitted secure protocols on the WAN	
	DS-1.3	Place externally accessible servers (e.g., web servers) within the DMZ.		DS-1.3	Place externally accessible servers (e.g., secure FTP server, web servers) within the DMZ	
	DS-1.4	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.		DS-1.4	Implement a process to patch network infrastructure devices (e.g., firewalls, routers, switches, etc.) regularly	
	DS-1.5	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.		DS-1.5	Harden network infrastructure devices based on security configuration standards	
	DS-1.6	Do not allow remote management of the firewall from any external interface(s).		DS-1.6	Do not allow remote access to WAN network infrastructure devices (e.g., firewall, router) that control access to content	

The Motion Picture of America Association (MPAA) has established a set of best practices for securely storing, processing and delivering protected media and content. For additional information on MPAA content security best practices refer to: http://www.fightfilmtheft.org/best-practice.html.

The table below was created by AWS to highlight the delta between the MPAA best practices published in 2013 and the MPAA best practices published in 2015.
- For any new control added to the 2015 MPAA best practices, see any rows highlighted in "green."
- For any control set which had a slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "blue."
- For any control set which was removed from the 2015 MPAA best practices, these controls were highlighted in "grey."
- Any control set which is not highlighted the requirements behind the controls were fundamentally unchanged.

MPAA Best Practices 2015			MPAA Best Practices 2013			AWS comments on the differences between 2015 and 2013 version
Security Topic	No.	Best Practice	Security Topic	No.	Best Practice	
	DS-1.7	Secure backups of network infrastructure/SAN/NAS devices and servers to a centrally secured server on the internal network.		DS-1.7	Secure backups of network infrastructure devices to a centrally secured server on the internal network	
	DS-1.8	Perform quarterly vulnerability scans of all external IP ranges and hosts at least and remediate issues.		DS-1.8	Perform an annual vulnerability scan on hosts that are externally accessible and remediate issues	
	DS-1.9	Perform annual penetration testing of all external IP ranges and hosts at least and remediate issues.		DS-1.9	Allow only authorized personnel to request the establishment of a connection with the telecom service provider	
	DS-1.10	Secure any point to point connections by using dedicated, private connections and by using encryption.				
	DS-1.11	Implement a synchronized time service protocol (e.g., Network Time Protocol) to ensure all systems have a common time reference.				
	DS-1.12	Establish, document and implement baseline security requirements for WAN network infrastructure devices and services.				
	DS-2.0	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.		DS-2.0	Prohibit Internet access on systems (desktops/ servers) that process or store digital content	The control requirements behind the control set did not change between 2015 and 2013.
Internet	DS-2.1	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 10 MB • Known domains that are sources of malware or viruses	Internet	DS-2.1	Implement e-mail filtering software or appliances that block the following from non-production networks: • Potential phishing e-mails • Prohibited file attachments (e.g., Visual Basic scripts, executables, etc.) • File size restrictions limited to 10 MB	
	DS-2.2	Implement web filtering software or appliances that restrict access to websites known for peer-to-peer file trading, viruses, hacking or other malicious sites.		DS-2.2	Implement web filtering software or appliances that restrict access to websites known for peer-to-peer file trading, viruses, hacking or other malicious sites	
	DS-3.0	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.		DS-3.0	Isolate the content/production network from non-production networks (e.g., office network, DMZ, etc.) by means of physical or logical network segmentation	2015 MPAA implemented additional controls regarding LAN / Internal Network: • Use switches/layer 3 devices to manage the network traffic, and disable all unused switch ports • Restrict the use of non-switched devices on the content/production network. • Disable SNMP if it is not in use • Harden systems • Conduct internal network vulnerability scans • Secure backups of local area network SAN/NAS, devices, servers and workstations to a centrally secured server on the internal network.
	DS-3.1	Restrict access to the content/production systems to authorized personnel.		DS-3.1	Restrict access to the content/production systems to authorized personnel	
	DS-3.2	Restrict remote access to the content/production network to only approved personnel who require access to perform their job responsibilities.		DS-3.2	Restrict remote access to the content/production network to only approved personnel who require access to perform their job responsibilities	
	DS-3.3	Use switches/layer 3 devices to manage the network traffic, and disable all unused switch ports on the content/production network to prevent packet sniffing by unauthorized devices.		DS-3.3	Disable all unused switch ports on the content/production network to prevent packet sniffing by unauthorized devices	
	DS-3.4	Restrict the use of non-switched devices such as hubs and repeaters on the content/production network.		DS-3.4	Restrict the use of non-switched devices such as hubs and repeaters on the content/production network	
LAN / Internal Network	DS-3.5	Prohibit dual-homed networking (physical networked bridging) on computer systems within the content/production network.	LAN	DS-3.5	Prohibit dual-homed networking (network bridging) on computer systems within the content/production network	
	DS-3.6	Implement a network-based intrusion detection /prevention system (IDS/IPS) on the content/production network.		DS-3.6	Implement a network-based intrusion detection or prevention system on the content/production network	
	DS-3.7	Disable SNMP (Simple Network Management Protocol) if it is not in use or uses only SNMPv3 or higher and select SNMP community strings that are strong passwords.				
	DS-3.8	Harden systems prior to placing them in the LAN / Internal Network.				
	DS-3.9	Conduct internal network vulnerability scans and remediate any issues, at least annually.				
	DS-3.10	Secure backups of local area network SAN/NAS, devices, servers and workstations to a centrally secured server on the internal network.				
	DS-4.0	Prohibit wireless networking and the use of wireless devices on the content/production network.		DS-4.0	Prohibit wireless networking and the use of wireless devices on the production/content network	The control requirements behind the control set did not change between 2015 and 2013.
	DS-4.1	Configure non-production wireless networks (e.g., administrative and guest) with the following security controls: • Disable WEP / WPA • Only Enable AES128 encryption (WPA2), or higher • Segregate "guest" networks from the company's other networks • Change default administrator logon credentials • Change default network name (SSID)		DS-4.1	Configure non-production wireless networks (e.g., administrative and guest) with the following security controls: • Disable WEP • Enable AES encryption • Segregate "guest" networks from the company's other networks	
Wireless/WLAN			Wireless			
	DS-4.2	Implement a process to scan for rogue wireless access points and remediate any validated issues.		DS-4.2	Implement a process to scan for rogue wireless access points annually	
	DS-5.0	Designate specific systems to be used for content input/output (I/O).		DS-5.0	Designate specific systems to be used for content input/output (I/O)	2015 MPAA removed the requirement to restrict the installation and or/use of media burners.
	DS-5.1	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.		DS-5.1	Block input/output (I/O) devices (e.g., USB, FireWire, e-SATA, SCSI, etc.) on all systems that handle or store content, with the exception of systems used for content I/O	
I/O Device Security			I/O Device Security	DS-5.2	Restrict the installation and/or use of media burners (e.g., DVD, Blu-ray, CD burners) and other devices with output capabilities to specific I/O systems used for outputting content to physical media	
	DS-6.0	Install anti-virus and anti-malware software on all workstations, servers, and on any device that connects to SAN/NAS systems.		DS-6.0	Install anti-virus software on all workstations and servers	2015 MPAA requires a inventory of system components and a documented network topology.
	DS-6.1	Update all anti-virus and anti-malware definitions daily, or more frequently.		DS-6.1	Update anti-virus definitions daily	
	DS-6.2	Scan all content for viruses and malware prior to ingest onto the content/production network.		DS-6.2	Scan file-based content for viruses prior to ingest onto the content/production network	
	DS-6.3	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		DS-6.3	Performing virus scans as follows: • Enable regular full system virus scanning on all workstations • Enable full system virus scans for servers, where applicable (e.g., non-SAN systems)	
	DS-6.4	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.		DS-6.4	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	
	DS-6.5	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.		DS-6.5	Prohibit users from being Administrators on their own workstations	
System Security			System Security			
	DS-6.6	Use cable locks on portable computing devices that handle content (e.g., laptops, tablets, towers) when they are left unattended.		DS-6.6	Use cable locks on portable computing devices that handle content (e.g., laptops, tablets, towers) when they are left unattended	
	DS-6.7	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.		DS-6.7	Install remote-kill software on all portable computing devices that handle content to allow remote wiping of hard drives and other storage devices	
	DS-6.8	Restrict software installation privileges to IT management.		DS-6.8	Restrict software installation privileges to approved users	
	DS-6.9	Implement security baselines and standards to configure systems (e.g., laptops, workstations, servers, SAN/NAS) that are set up internally.		DS-6.9	Implement security baselines and standards to configure systems (e.g., laptops, workstations, servers) that are set up internally	
	DS-6.10	Unnecessary services and applications should be uninstalled from content transfer servers.		DS-6.10	Unnecessary services and applications should be uninstalled from content transfer servers	
	DS-6.11	Maintain an inventory of systems and system components.				
	DS-6.12	Document the network topology and update the diagram annually or when significant changes are made to the infrastructure.				
	DS-7.0	Establish and implement an account management process for administrator, user, and service accounts for all information systems and applications that handle content.		DS-7.0	Establish and implement an account management process for administrator, user, and service accounts for all information systems and applications that handle content	The control requirements behind the control set did not change between 2015 and 2013.
	DS-7.1	Maintain traceable evidence of the account management activities (e.g., approval emails, change request forms).		DS-7.1	Maintain traceable evidence of the account management activities (e.g., approval e-mails, change request forms)	

The Motion Picture of America Association (MPAA) has established a set of best practices for securely storing, processing and delivering protected media and content. For additional information on MPAA content security best practices refer to: http://www.fightfilmtheft.org/best-practice.html.

The table below was created by AWS to highlight the delta between the MPAA best practices published in 2013 and the MPAA best practices published in 2015.
- For any new control added to the 2015 MPAA best practices, see any rows highlighted in "green."
- For any control set which had a slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "blue."
- For any control set which was removed from the 2015 MPAA best practices, these controls were highlighted in "grey."
- Any control set which is not highlighted the requirements behind the controls were fundamentally unchanged.

MPAA Best Practices 2015			MPAA Best Practices 2013			AWS comments on the differences between 2015 and 2013 version
Security Topic	No.	Best Practice	Security Topic	No.	Best Practice	
Account Management	DS-7.2	Assign unique credentials on a need-to-know basis using the principles of least privilege.	Account Management	DS-7.2	Assign unique credentials on a need-to-know basis using the principles of least privilege	
	DS-7.3	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).		DS-7.3	Rename the default administrator accounts and limit the use of these accounts to special situations that require these credentials (e.g., operating system updates, patch installations, software updates)	
	DS-7.4	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).		DS-7.4	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)	
	DS-7.5	Monitor and audit administrator and service account activities.		DS-7.5	Monitor and audit administrator and service account activities	
	DS-7.6	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.		DS-7.6	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	
	DS-7.7	Restrict user access to content on a per-project basis.		DS-7.7	Review user access to content on a per-project basis	
	DS-7.8	Disable or remove local accounts on systems that handle content where technically feasible.		DS-7.8	Disable or remove local accounts on systems that handle content where technically feasible	
Authentication	DS-8.0	Enforce the use of unique usernames and passwords to access information systems.	Authentication	DS-8.0	Enforce the use of unique usernames and passwords to access information systems	2015 MPAA suggest the provider implement additional authentication mechanisms, which would provide a layered authentication strategy.
	DS-8.1	Enforce a strong password policy for gaining access to information systems.		DS-8.1	Enforce a strong password policy for gaining access to information systems	
	DS-8.2	Implement two-factor authentication (e.g., username/password and hard token) for remote access (e.g., VPN) to the networks.		DS-8.2	Implement two-factor authentication (e.g., username/password and hard token) for remote access (e.g., VPN) to the networks.	
	DS-8.3	Implement password-protected screensavers or screen-lock software for servers and workstations.		DS-8.3	Implement password-protected screensavers or screen-lock software for servers and workstations	
	DS-8.4	Consider implementing additional authentication mechanisms to provide a layered authentication strategy for WAN and LAN / Internal Network access.				
Logging and Monitoring	DS-9.0	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)	Logging and Monitoring	DS-9.0	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)	2015 MPAA updated the requirement for log storage to 1 year vs. 6 months. As well as, the requirement to manage the logs in a central repository.
	DS-9.1	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.S-9.0	Implement logging mechanisms on all systems used for: • Key generation • Key management • Vendor certificate management	
	DS-9.2	Configure logging systems to send automatic notifications when security events are detected in order to facilitate active response to incidents.		DS-9.1	Configure logging systems to send automatic notifications when security events are detected in order to facilitate active response to incidents	
	DS-9.3	Investigate any unusual activity reported by the logging and reporting systems.		DS-9.2	Investigate any unusual activity reported by the logging and reporting systems	
	DS-9.4a	Implement logging mechanisms on all systems used for the following: • Key generation • Key management • Vendor certificate management		DS-9.3	Review logs weekly	
	DS-9.4b	Review all logs weekly, and review all critical and high daily.		DS-9.4	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-9.5	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-9.5	Retain logs for at least 6 months	
	DS-9.6	Retain logs for at least one year.		DS-9.6	Restrict log access to appropriate personnel	
	DS-9.7	Restrict log access to appropriate personnel.		DS-9.7	Send automatic notifications to the production coordinator(s) upon outbound content transmission	
Mobile Security	DS-10.0	Develop a BYOD (Bring Your Own Device) policy for mobile devices accessing or storing content.				2015 MPAA added this control set.
	DS-10.1	Develop a list of approved applications, application stores, and application plugins/extensions for mobile devices accessing or storing content.				
	DS-10.2	Maintain an inventory of all mobile devices that access or store content.				
	DS-10.3	Require encryption either for the entire device or for areas of the device where content will be handled or stored.				
	DS-10.4	Prevent the circumvention of security controls.				
	DS-10.5	Implement a system to perform a remote wipe of a mobile device, should it be lost / stolen / compromised or otherwise necessary.				
	DS-10.6	Implement automatic locking of the device after 10 minutes of non-use.				
	DS-10.7	Manage all mobile device operating system patches and application updates.				
	DS-10.8	Enforce password policies.				
	DS-10.9	Implement a system to perform backup and restoration of mobile devices.				
Security Techniques	DS-11.0	Ensure that security techniques (e.g., spoiling, invisible/visible watermarking) are available for use and are applied when instructed.	Security Techniques/Advanced Security Techniques	DS-10.0	Ensure that security techniques (e.g., spoiling, invisible/visible watermarking) are available for use and are applied when instructed	2015 MPAA added controls around the encryption of content at rest and in motion. Additionally, procedures around the storage of public and private keys.
	DS-11.1	Encrypt content on hard drives or encrypt entire hard drives using a minimum of AES 128-bit, or higher, encryption by either: • File-based encryption: (i.e., encrypting the content itself) • Drive-based encryption: (i.e., encrypting the hard drive)		DS.S-10.0	Implement a process for key management that addresses the following: • Approval and revocation of trusted devices • Generation, renewal, and revocation of content keys • Internal and external distribution of content keys	
	DS-11.2	Send decryption keys or passwords using an out-of-band communication protocol (i.e., not on the same storage media as the content itself).		DS-10.1	Encrypt content on hard drives using a minimum of AES 128-bit encryption by either: • File-based encryption: (i.e., encrypting the content itself) • Drive-based encryption: (i.e., encrypting the hard drive)	
	DS-11.3	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		DS.S-10.1	Confirm that devices on the Trusted Devices List (TDL) are appropriate based on rights owners' approval	
	DS-11.4	Encrypt content at rest and in motion, including across virtual server instances, using a minimum of AES 128-bit, or higher, encryption.		DS-10.2	Send decryption keys or passwords using an out-of-band communication protocol (i.e., not on the same storage media as the content itself)	

The Motion Picture of America Association (MPAA) has established a set of best practices for securely storing, processing and delivering protected media and content. For additional information on MPAA content security best practices refer to: http://www.fightfilmtheft.org/best-practice.html.

The table below was created by AWS to highlight the delta between the MPAA best practices published in 2013 and the MPAA best practices published in 2015.
- For any new control added to the 2015 MPAA best practices, see any rows highlighted in "green."
- For any control set which had a slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "blue."
- For any control set which was removed from the 2015 MPAA best practices, these controls were highlighted in "grey."
- Any control set which is not highlighted the requirements behind the controls were fundamentally unchanged.

MPAA Best Practices 2015			MPAA Best Practices 2013			AWS comments on the differences between 2015 and 2013 version
Security Topic	**No.**	**Best Practice**	**Security Topic**	**No.**	**Best Practice**	
	DS-11.5	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) o Has at least two full-length key components or key shares, in accordance with a security industry accepted method		DS.S-10.2	Confirm the validity of content keys and ensure that expiration dates conform with client instructions	
	DS-11.6	Confirm that devices on the Trusted Devices List (TDL) are appropriate based on rights owners' approval.				
	DS-11.7	Confirm the validity of content keys and ensure that expiration dates conform to client instructions.				
	DS-12.0	Implement a digital content management system to provide detailed tracking of digital content.				2015 MPAA added this control set.
	DS-12.1	Retain digital content movement transaction logs for one year.				
Content Tracking	DS-12.2	Review logs from digital content management system periodically and investigate anomalies.				
	DS-12.3	Use client AKAs ("aliases") when applicable in digital asset tracking systems.				
	DS-13.0	Use only client-approved transfer systems that utilize access controls, a minimum of AES 128-bit, or higher, encryption for content at rest and for content in motion and use strong authentication for content transfer sessions.				2015 MPAA added this control set.
Transfer Systems	DS-13.1	Implement an exception process, where prior client approval must be obtained in writing, to address situations where encrypted transfer tools are not used.				
	DS-14.0	Implement and use dedicated systems for content transfers.		DS-12.0	Implement and use dedicated systems for content transfers	2015 MPAA added a control around sending automatic notificaiton for content transmition.
	DS-14.1	Separate content transfer systems from administrative and production networks.		DS-12.1	Segment systems dedicated to transfer files from systems that store or process content and from the non-production network	
	DS-14.2	Place content transfer systems in a Demilitarized Zone (DMZ) and not in the content/production network.		DS-12.2	Place content transfer systems in a Demilitarized Zone (DMZ) and not in the content/production network	
Transfer Device Methodology	DS-14.3	Remove content from content transfer devices/systems immediately after successful transmission/receipt.	Transfer Device Methodology	DS-12.3	Remove content from content transfer devices immediately after successful transmission/receipt	
	DS-14.4	Send automatic notifications to the production coordinator(s) upon outbound content transmission.				
	DS-15.0	Restrict access to web portals which are used for transferring content, streaming content and key distribution to authorized users.		DS-13.0	Restrict access to web portals which are used for transferring content, streaming content and key distribution to authorized users	2015 MPAA added a control around annual penetration testing of web applications.
	DS-15.1	Assign unique credentials (e.g., username and password) to portal users and distribute credentials to clients securely.		DS-13.1	Assign unique credentials (e.g., username and password) to portal users and distribute credentials to clients securely	
	DS-15.2	Ensure users only have access to their own digital assets (i.e., client A must not have access to client B's content).		DS-13.2	Ensure users only have access to their own digital assets (i.e., client A must not have access to client B's content)	
	DS-15.3	Place the web portal on a dedicated server in the DMZ and limit access to/from specific IPs and protocols.		DS-13.3	Place the web portal on a dedicated server in the DMZ and limit access to/from specific IPs and protocols	
	DS-15.4	Prohibit the use of third-party production software/systems/services that are hosted on an internet web server unless approved by client in advance.		DS-13.4	Prohibit the use third-party production tracking software that is hosted on internet web server unless approved by client	
Client Portal	DS-15.5	Use HTTPS and enforce use of a strong cipher suite (e.g., TLS v1) for the internal/external web portal.	Client Portal	DS-13.5	Use HTTPS and enforce use of a strong cipher suite (e.g.,SSLv3 or TLS v1) for the internal/external web portal	
	DS-15.6	Do not use persistent cookies or cookies that store credentials in plaintext.		DS-13.6	Do not use persistent cookies or cookies that store credentials in plaintext	
	DS-15.7	Set access to content on internal or external portals to expire automatically at predefined intervals, where configurable.		DS-13.7	Set access to content on internal or external portals to expire automatically at predefined intervals, where configurable	
	DS-15.8	Test for web application vulnerabilities quarterly and remediate any validated issues.		DS-13.8	Test for web application vulnerabilities annually	
	DS-15.9	Perform annual penetration testing of web applications and remediate any validated issues.		DS-13.9	Allow only authorized personnel to request the establishment of a connection with the telecom service provider	
	DS-15.10	Allow only authorized personnel to request the establishment of a connection with the telecom service provider.		DS-13.10	Prohibit transmission of content using e-mail (including webmail) from the non-production network, and manage exceptions using the exception policy	
	DS-15.11	Prohibit transmission of content using email (including webmail).		DS-13.11	Review access to the client web portal at least quarterly	
	DS-15.12	Review access to the client web portal at least quarterly.				
				DS-11.0	Implement transfer tools that use access controls, a minimum of AES 128-bit encryption and strong authentication for content transfer sessions	2015 MPAA removed these controls.
			Transfer Tools			
				DS-11.1	Implement an exception process, where client prior approval must be obtained in writing, to address situations where encrypted transfer tools are not used	