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.

Media Companies can utilize these best practices as a way to assess risk and audit security of the content management.

The table below documents AWS alignment with Motion Picture of America Association (MPAA) Content Security Model Guidelines released April 2, 2015. For additional information a reference to AWS third-party audited certifications and reports is provided.

* The ISO 27002 and NIST 800-53 mapping is captured as defined in the *"MPAA Content Security Best Practices Common Guidelines April 2, 2015"*

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
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.	The Control environment at Amazon begins at the highest level of the Company. Executive and senior leadership play important roles in establishing the Company's tone and core values. Every employee is provided with the Company's Code of Business Conduct and Ethics and completes periodic training. Compliance audits are performed so that employees understand and follow established policies. Refer to AWS Risk & Compliance whitepaper for additional details - available at	SOC1 1.1 SOC1 1.2 SOC2 9.1	5.1.2 6.1.1	12.1 12.4 12.5	AT-2 AT-3 PM-1 PM-2 PM-6
Executive Security Awareness/ Oversight	MS-1.1	Review information security management policies and processes at least annually.					
Executive Security Awareness/ Oversight	MS-1.2	Train and engage executive management/owner(s) on the business' responsibilities to protect content at least annually.					
Executive Security Awareness/ Oversight	MS-1.3	Create an information security management group to establish and review information security management policies.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			http://aws.amazon.com/security.				
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.	AWS has implemented a formal, documented risk assessment policy that is updated and reviewed at least annually. This policy addresses purpose, scope, roles, responsibilities, and management commitment. In alignment with this policy, an annual risk assessment which covers all AWS regions and businesses is conducted by the AWS Compliance team and reviewed by AWS Senior Management. This is in addition to the Certification, attestation and reports that are conducted by independent auditors. The purpose of the risk assessment is to identify threats and vulnerabilities of AWS, to assign the threats and vulnerabilities a risk rating, to formally document the assessment, and to create a risk treatment plan for addressing issues. Risk	SOC1 1.2 SOC2 9.3	5.1.2 6.1.1 6.1.3	12.1 12.2	CA-1 RA-1 RA-2
Risk Management	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.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			assessment results are reviewed by the AWS Senior Management on an annual basis and when a significant change warrants a new risk assessment prior to the annual risk assessment. Customers retain ownership of their data (content) and are responsible for assessing and managing risk associated with the workflows of their data to meet their compliance needs. The AWS Risk Management framework is reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.				
Security Organization	MS-3.0	Identify security key point(s) of contact and formally define roles and responsibilities for content and asset protection.	AWS has an established information security organization managed by the AWS Security team and is led by the AWS Chief Information Security Officer (CISO). AWS maintains and provides security awareness training to all information	SOC1 1.1	6.1.3	12.4 12.5	PM-2

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			system users supporting AWS. This annual security awareness training includes the following topics; The purpose for security and awareness training, The location of all AWS policies, AWS incident response procedures (including instructions on how to report internal and external security incidents). Systems within AWS are extensively instrumented to monitor key operational and security metrics. Alarms are configured to automatically notify operations and management personnel when early warning thresholds are crossed on key metrics. When a threshold is crossed, the AWS incident response process is initiated. The Amazon Incident Response team employs industry-standard diagnostic procedures to drive resolution during business-impacting events. Staff				

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			operates 24x7x365 coverage to detect incidents and manage the impact to resolution. AWS roles & Responsibilities are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.				
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	AWS has established an information security framework and policies based on the Control Objectives for Information and related Technology (COBIT) framework and have effectively integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, the PCI DSS v3.0 and the National Institute of Standards and Technology (NIST) Publication 800-53 (Recommended Security Controls for Federal Information Systems).	SOC1 1.2 SOC2 9.1 SOC2 9.4	5.1.1 5.1.2 6.1.1 8.1.3 8.2.2	1.1 1.5 2.5 3.1 3.7 4.3 5.4 6.7 7.3 8.1 8.4 8.8 9.10 10.8 11.6 12.1 12.3 12.4	AT-1 AT-2 AT-3 AT-4 PL-1 PS-7

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
		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)	AWS maintains and provides security awareness training to all information system users supporting AWS. This annual security awareness training includes the following topics; the purpose for security and awareness training, the location of all AWS policies, AWS incident response procedures (including instructions on how to report internal and external security incidents). AWS policies, procedures and relevant training programs are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance AWS Third-Party Attestations, Reports and Certifications mapping to Best Practice.				
Policies and Procedures	MS-4.1	Review and update security policies and procedures at least annually.					
Policies and Procedures	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.					
Policies and Procedures	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 Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
		· Security incident reporting and escalation · Disciplinary policy · Encryption and key management for all individuals who handle encrypted content · Asset disposal and destruction processes					
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.	AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment. AWS utilizes a three-phased approach to manage incidents: 1. Activation and Notification Phase: Incidents for AWS begin with the detection of an event. This can come from several sources including: a. Metrics and alarms - AWS maintains an exceptional situational awareness capability, most issues are rapidly detected from 24x7x365 monitoring and alarming of real time metrics	SOC1 8.1 SOC1 8.2	16.1.1 16.1.2	10.6 12.1	IR-1 IR-2 IR-4 IR-5 IR-6 IR-7 IR-8
Incident Response	MS-5.1	Identify the security incident response team who will be responsible for detecting, analyzing, and remediating security incidents.					
Incident Response	MS-5.2	Establish a security incident reporting process for individuals to report detected incidents to the security incident response team.					
Incident Response	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.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			and service dashboards. The majority of incidents are detected in this manner. AWS utilizes early indicator alarms to proactively identify issues that may ultimately impact Customers. b. Trouble ticket entered by an AWS employee c. Calls to the 24X7X365 technical support hotline. If the event meets incident criteria, then the relevant on-call support engineer will start an engagement utilizing AWS Event Management Tool system to start the engagement and page relevant program resolvers (e.g. Security team). The resolvers will perform an analysis of the incident to determine if additional resolvers should be engaged and to determine the approximate root cause. 2. Recovery Phase - the relevant resolvers will perform break fix to address the incident. Once				

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			troubleshooting, break fix and affected components are addressed, the call leader will assign next steps in terms of follow-up documentation and follow-up actions and end the call engagement. 3. Reconstitution Phase - Once the relevant fix activities are complete the call leader will declare that the recovery phase is complete. Post mortem and deep root cause analysis of the incident will be assigned to the relevant team. The results of the post mortem will be reviewed by relevant senior management and relevant actions such as design changes etc. will be captured in a Correction of Errors (COE) document and tracked to completion. In addition to the internal communication mechanisms detailed above, AWS has also implemented various methods of external				

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			communication to support its customer base and community. Mechanisms are in place to allow the customer support team to be notified of operational issues that impact the customer experience. A "Service Health Dashboard" is available and maintained by the customer support team to alert customers to any issues that may be of broad impact. AWS incident management program reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.				
Business Continuity & Disaster Recovery	MS-6.0	Establish a formal plan that describes actions to be taken to ensure business continuity.	AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment. AWS utilizes a three-phased approach to manage incidents:	SOC1 8.1 SOC1 8.2 SOC2 10.3	17.1.1		CP
Business Continuity & Disaster Recovery	MS-6.1	Identify the business continuity team who will be responsible for detecting, analyzing and remediating continuity incidents.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			1. Activation and Notification Phase: Incidents for AWS begin with the detection of an event. This can come from several sources including: a. Metrics and alarms - AWS maintains an exceptional situational awareness capability, most issues are rapidly detected from 24x7x365 monitoring and alarming of real time metrics and service dashboards. The majority of incidents are detected in this manner. AWS utilizes early indicator alarms to proactively identify issues that may ultimately impact Customers. b. Trouble ticket entered by an AWS employee c. Calls to the 24X7X365 technical support hotline. If the event meets incident criteria, then the relevant on-call support engineer will start an engagement utilizing AWS Event Management Tool system to start the				

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			engagement and page relevant program resolvers (e.g. Security team). The resolvers will perform an analysis of the incident to determine if additional resolvers should be engaged and to determine the approximate root cause. 2. Recovery Phase - the relevant resolvers will perform break fix to address the incident. Once troubleshooting, break fix and affected components are addressed, the call leader will assign next steps in terms of follow-up documentation and follow-up actions and end the call engagement. 3. Reconstitution Phase - Once the relevant fix activities are complete the call leader will declare that the recovery phase is complete. Post mortem and deep root cause analysis of the incident will be assigned to the relevant team. The				

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			results of the post mortem will be reviewed by relevant senior management and relevant actions such as design changes etc. will be captured in a Correction of Errors (COE) document and tracked to completion. In addition to the internal communication mechanisms detailed above, AWS has also implemented various methods of external communication to support its customer base and community. Mechanisms are in place to allow the customer support team to be notified of operational issues that impact the customer experience. A "Service Health Dashboard" is available and maintained by the customer support team to alert customers to any issues that may be of broad impact.				
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.	AWS applies a systematic approach to managing changes to ensure changes to customer-impacting aspects of a service are	SOC1 6.1	14.2.2	6.4	CM

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			reviewed, tested and approved. AWS's change management procedures have been developed in alignment with ISO 27001 standard. The AWS SOC 1 Type 2 report provides details on the specific control activities executed by AWS.				
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 documentation of Content (data) is the responsibility of AWS Customers as Customers retain ownership and control of their own guest operating systems, software, applications and data.		11.1		
Workflow	MS-8.1	Update the workflow when there are changes to the process, and review the workflow process at least annually to identify changes.					
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 of Workflow of Content (data) is the responsibility of AWS Customers as Customers retain ownership and control of their own guest operating systems, software, applications and data.		6.1.2		

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
Background Checks	MS-10.0	Perform background screening checks on all company personnel and third party workers.	AWS conducts criminal background checks, as permitted by applicable law, as part of pre-employment screening practices for employees commensurate with the employee's position and level of access to AWS facilities. AWS background check program is reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.	SOC 2 9.5	7.1.1	12.7	PS-3
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.	Amazon Legal Counsel manages and periodically revises the Amazon Non-Disclosure Agreement (NDA) to reflect AWS business needs. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.		7.1.2 8.1.4		PL-4 PS-6 PS-8 PS-4 PS-6 PS-8 SA-9
Confidentiality Agreements	MS-11.1	Require all company personnel to return all content and client information in their possession upon termination of their employment or contract.					
Third Party Use and Screening	MS-12.0	Require all third party workers (e.g., freelancers) who handle content to	As part of the on-boarding process, all personnel	SOC1 5.11 SOC1 5.12	7.1.1 7.1.2	2.6 12.6	PL-4 PS-4

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
		sign confidentiality agreements (e.g., non-disclosure) upon engagement.	supporting AWS systems and devices sign a non-disclosure agreement prior to being granted access. Additionally, as part of orientation, personnel are required to read and accept the Acceptable Use Policy and the Amazon Code of Business Conduct and Ethics (Code of Conduct) Policy. Personnel security requirements for third-party providers supporting AWS systems and devices are established in a Mutual Non-Disclosure Agreement between AWS' parent organization, Amazon.com, and the respective third-party provider. The Amazon Legal Counsel and the AWS Procurement team define AWS third party provider personnel security requirements in contract agreements with the third party provider. All persons working with AWS information must at a minimum, meet the screening process for pre-		7.2.1 8.1.4 11.1.2	12.8 12.9	PS-6 PS-7 SA-9
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-12.2	Include security requirements in third party contracts.					
Third Party Use and Screening	MS-12.3	Implement a process to reclaim content when terminating relationships.					
Third Party Use and Screening	MS-12.4	Require third party workers to be bonded and insured where appropriate (e.g., courier service).					
Third Party Use and Screening	MS-12.5	Restrict third party access to content/production areas unless required for their job function.					
Third Party Use and Screening	MS-12.6	Notify clients if subcontractors are used to handle content or work is offloaded to another company.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			employment background checks and sign a Non-Disclosure Agreement (NDA) prior to being granted access to AWS information. AWS Third Party requirements are reviewed by independent external auditors during audits for our PCI DSS, ISO 27001 and FedRAMP compliance.				
Entry/Exit Points	PS-1.0	Secure all entry/exit points of the facility at all times, including loading dock doors and windows.	AWS data centers are housed in nondescript facilities and are not open to the public. Physical access is strictly controlled both at the perimeter and at building ingress points. AWS only provides data center access and information to vendors, contractors, and visitors who have a legitimate business need for such privileges, such as emergency repairs. All visitors to data centers must be pre-authorized by the applicable Area Access Manager (AAM) and documented in AWS ticket management system. When	SOC1 5.1 SOC1 5.6	11.1	9.1	PE-1 PE-2 PE-3 PE-6
Entry/Exit Points	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).					
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					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
		· All tenants within the facility must be reported to client prior to engagement	they arrive at the data center, they must present identification and sign in before they are issued a visitor badge. They are continually escorted by authorized staff while in the data center. AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.				
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	AWS data centers are housed in nondescript facilities and are not open to the public. Physical access is strictly controlled both at the perimeter and at building ingress points. AWS only provides data center access and information to vendors, contractors, and visitors who have a legitimate business need for such privileges, such as emergency repairs. All visitors to data centers must be pre-authorized by the applicable Area Access	SOC1 5.1 SOC1 5.4	11.1	9.1 9.2 9.4	PE-2 PE-3 PE-7
Visitor Entry/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.					
Visitor Entry/Exit	PS-2.2	Do not provide visitors with key card access to content/production areas.					
Visitor Entry/Exit	PS-2.3	Require visitors to be escorted by authorized employees while on-site, or in content/production areas.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			Manager (AAM) and documented in AWS ticket management system. When they arrive at the data center, they must present identification and sign in before they are issued a visitor badge. They are continually escorted by authorized staff while in the data center. AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.				
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.	AWS provides personnel with approved long term data center access an electronic access card with photographic identification. AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.	SOC1 5.1	11.1	9.1 9.2 9.4	PE-3
Perimeter Security	PS-4.0	Implement perimeter security controls that address risks that the facility may	Physical access to data centers is enforced by AWS's	SOC1 5.1 SOC1 5.4	11.1	9.1	PE-3

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
		be exposed to as identified by the organization's risk assessment.	electronic access control system, which is comprised of card readers and PIN pads for building and room ingress and card readers only for building and room egress. Enforcing the use of card readers for building and room egress provides anti-passback functionality to help ensure that unauthorized individuals do not tailgate authorized Persons and get in without a badge. In addition to the access control system, all entrances to AWS data centers, including the main entrance, the loading dock, and any roof doors/hatches, are secured with intrusion detection devices that sound alarms if the door is forced open or held open. In addition to electronic mechanisms, AWS data centers utilize trained security guards 24x7, who are stationed in and around the building.				
Perimeter Security	PS-4.1	Place security guards at perimeter entrances and non- emergency entry/exit points.					
Perimeter Security	PS-4.2	Implement a daily security patrol process with a randomized schedule and document the patrol results in a log.					
Perimeter Security	PS-4.3	Lock perimeter gates at all times.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			Access to data centers within the system boundary is granted on a need-to-know basis only, with all physical access requests being reviewed and approved by the appropriate Area Access Manager (AAM). AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.				
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.).	All entrances to AWS data centers, including the main entrance, the loading dock, and any roof doors/hatches, are secured with intrusion detection devices that sound alarms and create an alarm in AWS centralized physical security monitoring too if a door is forced open or held open. In addition to electronic mechanisms, AWS data centers utilize trained security guards 24x7, who are stationed in and around the building. All alarms are	SOC1 5.1 SOC1 5.3 SOC1 5.6 SOC1 5.7	11.1	9.1	AC-6 PE-3 PE-6 PE-9 PE-10 PE-11 PE-13
Alarms	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.).					
Alarms	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					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
		than a pre-determined period of time (e.g., 60 seconds).	investigated by a security guard with root cause documented for all incidents. All alarms are set to auto-escalate if response does not occur within SLA time. Access to data centers within the system boundary is granted on a need-to-know basis only, with all physical access requests being reviewed and approved by the appropriate Area Access Manager (AAM). AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.				
Alarms	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.).					
Alarms	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.					
Alarms	PS-5.5	Review the list of users who can arm and disarm alarm systems quarterly, or upon change of personnel.					
Alarms	PS-5.6	Test the alarm system quarterly.					
Alarms	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.	Physical access to data centers is enforced by AWS's electronic access control system, which is comprised of card readers and PIN pads for building and room ingress and card readers only for building and room egress. Enforcing the use of card readers for building and	SOC 1 5.1 SOC 1 5.3	11.1	9.1 9.2 9.4	PE-2 PE-3
Authorization	PS-6.1	Restrict access to production systems to authorized personnel only.					
Authorization	PS-6.2	Review access to restricted areas (e.g., vault, server/machine room) quarterly and when the roles or employment					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
		status of company personnel and/or third party workers are changed.	room egress provides anti-passback functionality to help ensure that unauthorized individuals do not tailgate authorized Persons and get in without a badge. In addition to the access control system, all entrances to AWS data centers, including the main entrance, the loading dock, and any roof doors/hatches, are secured with intrusion detection devices that sound alarms if the door is forced open or held open. In addition to electronic mechanisms, AWS data centers utilize trained security guards 24x7, who are stationed in and around the building. Access to data centers is granted on a need-to-know basis only, with all physical access requests being reviewed and approved by the appropriate Area Access				

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			Manager (AAM). AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.				
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.	Physical access to data centers is enforced by AWS's electronic access control system, which is comprised of card readers and PIN pads for building and room ingress and card readers only for building and room egress. Enforcing the use of card readers for building and room egress provides anti-passback functionality to help ensure that unauthorized individuals do not tailgate authorized Persons and get in without a badge. The ability to create and print a badge is systematically enforced and restricted to a core set of security personnel. All badges are activated for a finite time period requiring re-approval prior to	SOC1 5.1 SOC1 5.3	11.1	9.1 9.2 9.4	PE-2 PE-3
Electronic Access Control	PS-7.1	Restrict electronic access system administration to appropriate personnel.					
Electronic Access Control	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.					
Electronic Access Control	PS-7.3	Disable lost electronic access devices (e.g., keycards, key fobs) in the system before issuing a new electronic access device.					
Electronic Access Control	PS-7.4	Issue third party access electronic access devices with a set expiration					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
		date (e.g. 90 days) based on an approved timeframe.	extension of badge expiration date. AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.				
Keys	PS-8.0	Limit the distribution of master keys and / or keys to restricted areas to authorized personnel only (e.g., owner, facilities management).	Physical security processes and procedures, including procedures for managing facility Master keys are owned, managed and executed by AWS physical security staff. AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.	SOC1 5.1	9.2.6 11.1	9.1	PE-2 PE-3 CM-5 CM-8
Keys	PS-8.1	Implement a check-in/check-out process to track and monitor the distribution of master keys and / or keys to restricted areas.					
Keys	PS-8.2	Use keys that can only be copied by a specific locksmith for exterior entry/exit points.					
Keys	PS-8.3	Inventory master keys and keys to restricted areas, including facility entry/exit points, quarterly.					
Keys	PS-8.4	Obtain all keys from terminated employees/third-parties or those who no longer need the access.					
Keys	PS-8.5	Implement electronic access control or rekey entire facility when master or sub-master keys are lost or missing.					
Cameras	PS-9.0	Install a CCTV system that records all facility entry/exit points and restricted areas (e.g. server/machine room, etc.).	Physical access is controlled both at the perimeter and at building ingress points by	SOC1 5.4	9.26 11.1	9.1	PE-2 PE-3

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
Cameras	PS-9.1	Review camera positioning and recordings to ensure adequate coverage, function, image quality, and lighting conditions and frame rate of surveillance footage at least daily.	professional security staff utilizing video surveillance, intrusion detection systems and other electronic means. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy. Images are retained for 90 days, unless limited to 30 days by legal or contractual obligations. AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.				CM-5 CM-8
Cameras	PS-9.2	Restrict physical and logical access to the CCTV console and to CCTV equipment (e.g., DVRs) to personnel responsible for administering/monitoring the system.					
Cameras	PS-9.3	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.					
Cameras	PS-9.4	Designate an employee or group of employees to monitor surveillance footage during operating hours and immediately investigate detected security incidents.					
Logging and Monitoring	PS-10.0	Log and review electronic access to restricted areas for suspicious events, at least weekly.	Physical access is controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems and other electronic means. All entrances to AWS data centers, including the main entrance, the loading dock,	SOC 1 5.1 SOC 1 5.4	12.4	9.1	AU-3 AU-6 AU-9 AU-11
Logging and Monitoring	PS-10.1	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					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
Logging and Monitoring	PS-10.2	Investigate suspicious electronic access activities that are detected.	and any roof doors/hatches, are secured with intrusion detection devices that sound alarms and create an alarm in AWS centralized physical security monitoring too if a door is forced open or held open. In addition to electronic mechanisms, AWS data centers utilize trained security guards 24x7, who are stationed in and around the building. All alarms are investigated by a security guard with root cause documented for all incidents. All alarms are set to auto-escalate if response does not occur within SLA time. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy. Images are retained for 90 days, unless limited to 30 days by legal or				
Logging and Monitoring	PS-10.3	Maintain an ongoing log of all confirmed electronic access incidents and include documentation of any follow-up activities that were taken.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			contractual obligations. AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.				
Searches	PS-11.0	Establish a policy, as permitted by local laws that allows security to randomly search persons, bags, packages, and personal items for client content.	In alignment with AWS Physical Security Policies, AWS reserves the right to execute a search of bags and packages in the event of an issue. AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.		11.1		
Searches	PS-11.1	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					
Searches	PS-11.2	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					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
		devices as part of the exit search procedure.					
Searches	PS-11.3	Enforce the use of transparent plastic bags and food containers for any food brought into production areas.					
Searches	PS-11.4	Implement a dress code policy that prohibits the use of oversized clothing (e.g., baggy pants, oversized hooded sweatshirts).					
Searches	PS-11.5	Use numbered tamper-evident stickers/holograms to identify authorized devices that can be taken in and out of the facility.					
Searches	PS-11.6	Implement a process to test the exit search procedure.					
Searches	PS-11.7	Perform a random vehicle search process when exiting the facility parking lot.					
Searches	PS-11.8	Segregate replication lines that process highly sensitive content and perform searches upon exiting segregated areas.					
Searches	PS-11.9	Implement additional controls to monitor security guards activity.					
Inventory Tracking	PS-12.0	Implement a content asset management system to provide detailed tracking of physical assets (i.e., received from client created at the facility).	Content Asset Management is owned, implemented and operated by AWS Customers. It is the responsibility of Customers to implement inventory tracking of their physical		8.1 8.2.2 8.2.3	9.9	AU-1 AU-3 AU-6 AU-9 AU-11 CM-8
Inventory Tracking	PS-12.1	Barcode or assign unique tracking identifier(s) to client assets and					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
		created media (e.g., tapes, hard drives) upon receipt and store assets in the vault when not in use.	assets. For AWS Data Center Environments, all new information system components, which include, but are not limited to, servers, racks, network devices, hard drives, system hardware components, and building materials that are shipped to and received by data centers require prior authorization by and notification to the Data Center Manager. Items are delivered to the loading dock of each AWS Data Center and are inspected for any damages or tampering with the packaging and signed for by a full-time employee of AWS. Upon shipment arrival, items are scanned and captured within the AWS Asset management system and device inventory tracking system. Once items are received, they are placed in an equipment storage room within the data center that				
Inventory Tracking	PS-12.2	Retain asset movement transaction logs for at least one year.					
Inventory Tracking	PS-12.3	Review logs from content asset management system at least weekly and investigate anomalies.					
Inventory Tracking	PS-12.4	Use studio film title aliases when applicable on physical assets and in asset tracking systems.					
Inventory Tracking	PS-12.5	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 Tracking	PS-12.6	Lock up and log assets that are delayed or returned if shipments could not be delivered on time.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			requires the swipe badge and PIN combination for access until they are installed on the data center floor. Prior to exiting the data center, items are scanned, tracked, and sanitized before authorization to leave the data center. AWS Asset Management processes and procedures are reviewed by independent external auditors during audits for our PCI DSS, ISO 27001 and FedRAMP compliance.				
Inventory Counts	PS-13.0	Perform a quarterly inventory count of each client's asset(s), reconcile against asset management records, and immediately communicate variances to clients.	Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to implement inventory tracking and monitoring of their physical assets. Internally, in alignment with ISO 27001 standards, AWS Hardware assets are assigned an owner, tracked and monitored by the AWS		6.1.2 8.1.1		AU-6 AC-5 CM-8
Inventory Counts	PS-13.1	Segregate duties between the vault staff and individuals who are responsible for performing inventory counts.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			personnel with AWS proprietary inventory management tools. Refer to ISO 27001 standard, Annex A, domain 7.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.				
Blank Media/ Raw Stock Tracking	PS-14.0	Tag (e.g., barcode, assign unique identifier) blank stock/raw stock per unit when received.	AWS customers retain control and ownership of their data and media assets. It is the responsibility of the Studio / Processing facility to manage security of media stock.		6.1.2 8.1.1		MP-4 PE-2 PE-3
Blank Media/ Raw Stock Tracking	PS-14.1	Establish a process to track consumption of raw materials (e.g., polycarbonate) monthly.					
Blank Media/ Raw Stock Tracking	PS-14.2	Store blank media/raw stock in a secured location.					
Client Assets	PS-15.0	Restrict access to finished client assets to personnel responsible for tracking and managing assets.	It is the responsibility of those individuals that screen / manage physical copies of finished assets to ensure that adequate physical security is implemented. As documented in MPAA PS-1 - PS-14 AWS operates a Physical Security Program and Asset Management	SOC1 5.1 SOC1 5.4	8.23	9.1 9.9	MP-2 MP-4 PE-2 PE-3
Client Assets	PS-15.1	Store client assets in a restricted and secure area (e.g., vault, safe, or other secure storage location).					
Client Assets	PS-15.2	Require two company personnel with separate access cards to unlock highly sensitive areas (e.g., safe, high-security cage) after-hours.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
Client Assets	PS-15.3	Use a locked fireproof safe to store undelivered packages that are kept at the facility overnight.	Program throughout all of our data centers that is regularly reviewed and assessed by independent third party auditors as a part of our continued SOC, PCI DSS, ISO 27001 and FedRAMP compliance program.				
Client Assets	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.					
Disposals	PS-16.0	Require that rejected, damaged, and obsolete stock containing client assets are erased, degaussed, shredded, or physically destroyed before disposal.	Customers retain responsibility to dispose of physical media assets per their own requirements. Internally, when an AWS storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. If a hardware device is unable		8.3.2	9.8	MP-6
Disposals	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.					
Disposals	PS-16.2	Maintain a log of asset disposal for at least 12 months.					
Disposals	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.					
Disposals	PS-16.4	Use automation to transfer rejected discs from replication machines					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
		directly into scrap bins (no machine operator handling).	to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.				
Shipping	PS-17.0	Require the facility to generate a valid work/shipping order to authorize client asset shipments out of the facility.	For AWS Data Center Environments, all new information system components, which include, but are not limited to, servers, racks, network devices, hard drives, system hardware components, and building materials that are shipped to and received by data centers require prior authorization by and notification to the Data Center Manager. Items are delivered to the loading dock of each AWS Data Center and are inspected for any damages or tampering with the packaging and signed for		8.3.3	9.9	AU-11 MP-5 PE-3 PE-7 PE-16
Shipping	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					
Shipping	PS-17.2	Secure client assets that are waiting to be picked up.					
Shipping	PS-17.3	Validate client assets leaving the facility against a valid work/shipping order.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
Shipping	PS-17.4	Prohibit couriers and delivery personnel from entering content/production areas of the facility.	by a full-time employee of AWS. Upon shipment arrival, items are scanned and captured within the AWS Asset management system and device inventory tracking system.				
Shipping	PS-17.5	Document and retain a separate log for truck driver information.					
Shipping	PS-17.6	Observe and monitor the on-site packing and sealing of trailers prior to shipping.					
Shipping	PS-17.7	Record, monitor and review travel times, routes, and delivery times for shipments between facilities.					
Shipping	PS-17.8	Prohibit the transfer of film elements other than for client studio approved purposes.					
Shipping	PS-17.9	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).	Once new information system components are received in the AWS Data Centers, they are placed in an equipment storage room within the data center that requires the swipe badge and PIN combination for access until they are installed on the data center floor. Prior to exiting the data center, items are scanned, tracked, and		8.2.3	9.9	MP-3 MP-4 MP-5 PE-16
Receiving	PS-18.1	Maintain a receiving log to be filled out by designated personnel upon receipt of deliveries.					
Receiving	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					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
		· Move the asset to the restricted area (e.g., vault, safe)	sanitized before authorization to leave the data center. AWS Asset Management processes and procedures are reviewed by independent external auditors during audits for our PCI DSS, ISO 27001 and FedRAMP compliance.				
Receiving	PS-18.3	Implement a secure method 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.	AWS Asset labels are customer agnostic and are utilized to maintain inventory of hardware within the AWS Asset Management Tool. Within AWS Data Centers hardware is not physically associated with a customer or the data stored on the hardware. All customer data, regardless of source is considered to be Critical, in turn, all media is treated as sensitive. AWS Asset Management processes and procedures are reviewed by independent external auditors during audits for		8.2.2	9.9	MP-3

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			our PCI DSS, ISO 27001 and FedRAMP compliance.				
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 of physical finished media assets are the responsibility of the relevant distributing body (such as companies involved with distribution, DVD Creation, Post-production etc.).		8.3.3		MP-5
Packaging	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)					
Packaging	PS-20.2	Apply shrink wrapping to all shipments, and inspect packaging before final shipment to ensure that it is adequately wrapped.					
Transport Vehicles	PS-21.0	Lock automobiles and trucks at all times, and do not place packages in clear view.	Transport of physical finished media assets (such as DVD's) are the responsibility of the relevant distributing body (such as companies involved with distribution, DVD Creation, Post-production etc.).				MP-5
Transport Vehicles	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					
Transport Vehicles	PS-21.2	Apply numbered seals on cargo doors for shipments of highly sensitive titles.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
Transport Vehicles	PS-21.3	Require security escorts to be used when delivering highly sensitive content to 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.	Boundary protection devices that employ rule sets, access control lists (ACL), and configurations enforce the flow of information between network fabrics. Several network fabrics exist at Amazon, each separated by devices that control the flow of information between fabrics. The flow of information between fabrics is established by approved authorizations, which exist as access control lists (ACL) which reside on these devices. These devices control the flow of information between fabrics as mandated by these ACLs. ACLs are defined, approved by appropriate personnel, managed and deployed using AWS ACL-manage tool. Amazon's Information Security team approves these ACLs. Approved firewall rule sets and access control lists between	SOC1 3.1 SOC1 3.4 SOC1 5.15 SOC1 8.1	9.1 10.1 12.1 12.2 12.3 12.4 12.6 13.1 13.2 16.1 17.1	1.1 1.2 1.3 1.4 5.1 5.2 5.3 10.1 10.2 10.3 10.4 11.2 11.3 12.5	AC-3 AC-4 AC-6 AC-17 AC-20 CA-3 CM-6 CM-7 RA-5 SC-7 SC-12 SC-33 SI-2
Firewall/WAN/ Perimeter Security	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.					
Firewall/WAN/ Perimeter Security	DS-1.2	Deny all protocols by default and enable only specific permitted secure protocols to access the WAN and firewall.					
Firewall/WAN/ Perimeter Security	DS-1.3	Place externally accessible servers (e.g., web servers) within the DMZ.					
Firewall/WAN/ Perimeter Security	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.					
Firewall/WAN/ Perimeter Security	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					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
		use or use only SNMPv3 or higher and select SNMP community strings that are strong passwords.	network fabrics restrict the flow of information to specific information system services. Access control lists and rule sets are reviewed and approved, and are automatically pushed to boundary protection devices on a periodic basis (at least every 24 hours) to ensure rule-sets and access control lists are up-to-date. AWS Network Management is regularly reviewed by independent third party auditors as a part of AWS ongoing compliance with SOC, PCI DSS, ISO 27001 and FedRAMP. AWS implements least privilege throughout its infrastructure components. AWS prohibits all ports and protocols that do not have a specific business purpose. AWS follows a rigorous approach to minimal implementation of only those features and functions that are essential to use of the device. Network				
Firewall/ WAN/ Perimeter Security	DS-1.6	Do not allow remote management of the firewall from any external interface(s).					
Firewall/ WAN/ Perimeter Security	DS-1.7	Secure backups of network infrastructure/SAN/NAS devices and servers to a centrally secured server on the internal network.					
Firewall/ WAN/ Perimeter Security	DS-1.8	Perform quarterly vulnerability scans of all external IP ranges and hosts at least and remediate issues.					
Firewall/ WAN/ Perimeter Security	DS-1.9	Perform annual penetration testing of all external IP ranges and hosts at least and remediate issues.					
Firewall/ WAN/ Perimeter Security	DS-1.10	Secure any point to point connections by using dedicated, private connections and by using encryption.					
Firewall/ WAN/ Perimeter Security	DS-1.11	Implement a synchronized time service protocol (e.g., Network Time Protocol) to ensure all systems have a common time reference.					
Firewall/ WAN/ Perimeter Security	DS-1.12	Establish, document and implement baseline security requirements for WAN network infrastructure devices and services.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			scanning is performed and any unnecessary ports or protocols in use are corrected. Regular internal and external vulnerability scans are performed on the host operating system, web application and databases in the AWS environment utilizing a variety of tools. Vulnerability scanning and remediation practices are regularly reviewed as a part of AWS continued compliance with PCI DSS and FedRAMP.				
Internet	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.	Boundary protection devices are configured in a deny-all mode. Boundary protection devices that employ rule sets, access control lists (ACL), and configurations enforce the flow of information between network fabrics. These devices are configured in deny-all mode, requiring an approved firewall set to allow for connectivity. Refer to DS-2.0 for additional	SOC1 3.1 SOC1 3.4 SOC1 3.14	7.1.3 11.2.2	1.1 1.2 1.3 1.4 2.2 5.1 6.6 8.5 11.2	CA-3 PL-4
Internet	DS-2.1	Implement email filtering software or appliances that block the following from non-production networks: · Potential phishing emails					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
		· 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	information on Management of AWS Network Firewalls. There is no inherent e-mail capability on AWS Assets and port 25 is not utilized. A Customer (e.g. studio, processing facility etc.) can utilize a system to host e-mail capabilities, however in that case it is the Customer's responsibility to employ the appropriate levels of spam and malware protection at e-mail entry and exit points and update spam and malware definitions when new releases are made available. Amazon assets (e.g. laptops) are configured with anti-virus software that includes e-mail filtering and malware detection. AWS Network Firewall management and Amazon's anti-virus program are reviewed by independent third party auditors as a part of AWS ongoing compliance				
Internet	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.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			with SOC, PCI DSS, ISO 27001 and FedRAMP.				
LAN / Internal Network	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.	AWS provides customers the ability to segment and manage networks but is not responsible for the implementation and operation of these segmented environments.		6.2 9.1 9.4 10.1 11.2 12.3 12.6 13.1 17.1		AC-18 SI-4
LAN / Internal Network	DS-3.1	Restrict access to the content/production systems to authorized personnel.					
LAN / Internal Network	DS-3.2	Restrict remote access to the content/production network to only approved personnel who require access to perform their job responsibilities.					
LAN / Internal Network	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.					
LAN / Internal 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 / Internal Network	DS-3.6	Implement a network-based intrusion detection /prevention system (IDS/IPS) on the content/production network.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
LAN / Internal 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.					
LAN / Internal Network	DS-3.8	Harden systems prior to placing them in the LAN / Internal Network.					
LAN / Internal Network	DS-3.9	Conduct internal network vulnerability scans and remediate any issues, at least annually.					
LAN / Internal Network	DS-3.10	Secure backups of local area network SAN/NAS, devices, servers and workstations to a centrally secured server on the internal network.					
Wireless/ WLAN	DS-4.0	Prohibit wireless networking and the use of wireless devices on the content/production network.	There is no inherent wireless capability on AWS Assets. Amazon assets (e.g. laptops) wireless capabilities are implemented and operated in alignment with industry standard secure wireless configuration standards. Amazon continuously monitors wireless networks in order to detect rouge devices. AWS management of Wireless networks is reviewed by independent third party auditors as a part of AWS ongoing compliance		9.1 13.1	11.1	AC-18 SI-4
Wireless/ WLAN	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)					
Wireless/ WLAN	DS-4.2	Implement a process to scan for rogue wireless access points and remediate any validated issues.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			with PCI DSS, ISO 27001 and FedRAMP.				
I/O Device Security	DS-5.0	Designate specific systems to be used for content input/output (I/O).	AWS prevents access to system output devices to only authorized persons. Access to obtain authorization requires the submission of an electronic request, providing a business case for access, and obtaining documented approval of that authorization by an Authorized Approver. AWS Access Management procedures are independently reviewed by a third party auditor as a part of continued compliance with SOC, PCI-DSS, ISO 27001 and FedRAMP. Personal electronic devices and removable media are prohibited from connecting to AWS information systems.	SOC 1 2.1 SOC 1 5.1	10.7.1	7.1 8.2	SC-7 AC-19 MP-2
I/O Device Security	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.					
System Security	DS-6.0	Install anti-virus and anti-malware software on all workstations, servers, and on any device that connects to SAN/NAS systems.	Within the AWS environment, a configuration management tool used to manage deployable software in packages, package groups,		6.2 8.1 9.4 10.1 11.1 12.2		SI-3 SI-2 RA-5 AC-5 SC-2 PE-3
System Security	DS-6.1	Update all anti-virus and anti-malware definitions daily, or more frequently.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
System Security	DS-6.2	Scan all content for viruses and malware prior to ingest onto the content/production network.	and environments. A package is a collection of related files, such as software, content, etc., that are tightly coupled. A package group is a set of packages that are often deployed together. An environment is the combination of a set of packages and package groups which are deployed to a set of host classes (hosts or servers that serve the same function). An environment represents the complete set of packages required for a server to fulfill a particular function. AWS maintains the baseline OS distribution used on hosts. All unneeded ports, protocols and services are disabled in the base builds. Service teams use the build tools to add only approved software packages necessary for the servers function per the configuration baselines maintained in the tools. Servers are regularly scanned and any		12.5 12.6 11.2 14.1 14.2		PE-5 MA-4 CM-10 CM-11 SI-7 AC-6 CM-7 CM-8
System Security	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					
System Security	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.					
System Security	DS-6.5	Prohibit users from being Administrators on their own workstations, unless required for software (e.g., Protocols, Clipster and authoring software such as Blu-Print, Scenarist and Toshiba). Documentation from the software provider must explicitly state that administrative rights are required.					
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.					
System Security	DS-6.7	Implement additional security controls for laptops and portable computing storage devices that contain content or sensitive information relating to					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
		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.	unnecessary ports or protocols in use are corrected using the flaw remediation process. Deployed software undergoes recurring penetration testing performed by carefully selected industry experts. Remediation of the penetration testing exercise is also incorporated into the baseline through the flaw remediation process. Amazon Information Security proactively monitors vendor's websites and other relevant outlets for new patches. Prior to implementation Patches are evaluated for security and operational impact and applied in timely manner based upon assessment. Amazon assets (e.g. laptops) are configured with anti-virus software that includes e-mail filtering and malware detection. AWS Configuration Management and Flaw				
System Security	DS-6.8	Restrict software installation privileges to IT management.					
System Security	DS-6.9	Implement security baselines and standards to configure systems (e.g., laptops, workstations, servers, SAN/NAS) that are set up internally.					
System Security	DS-6.10	Unnecessary services and applications should be uninstalled from content transfer servers.					
System Security	DS-6.11	Maintain an inventory of systems and system components.					
System Security	DS-6.12	Document the network topology and update the diagram annually or when significant changes are made to the infrastructure.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			Remediation Process are all reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP.				
Account Management	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.	AWS has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy). The policy addresses purpose, scope, roles, responsibilities and management commitment. AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. When user accounts are created, user accounts are created to have minimal access. Access above these least privileges requires appropriate authorization. Authorized users of AWS systems and devices are	SOC1 2.1 SOC1 2.2 SOC1 2.3 SOC1 2.4	8.1 9.1 9.2 9.4 12.1 12.4 18.2	7.1 8.1 8.2 10.6	AC-2 AC-6 AU-2 AU-3 AU-6 AU-12 IA-4 PS-4 PS-5 PE-2

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
Account Management	DS-7.1	Maintain traceable evidence of the account management activities (e.g., approval emails, change request forms).	provided access privileges via group membership specific to the authorized individuals job function and role. Conditions for group membership are established and verified by group owners. User, group, and system accounts all have unique identifiers and are not reused. Guest/anonymous and temporary accounts are not used and are not allowed on devices. User accounts are reviewed at least quarterly. On a quarterly basis, all group owners review and remove, as needed, any users who no longer require group membership. This review is initiated by a systematic notification sent to the group owner by the AWS Account Management Tool, which notifies the group owner to perform a baseline of the group. A baseline is a full re-evaluation of				
Account Management	DS-7.2	Assign unique credentials on a need-to-know basis using the principles of least privilege.					
Account Management	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).					
Account Management	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).					
Account Management	DS-7.5	Monitor and audit administrator and service account activities.					
Account Management	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.					
Account Management	DS-7.7	Restrict user access to content on a per-project basis.					
Account Management	DS-7.8	Disable or remove local accounts on systems that handle content where technically feasible.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			permissions by the group owner. If the baseline isn't completed by the deadline, all group members are removed. User accounts are automatically disabled systematically after 90 days of inactivity. AWS have identified auditable event categories across systems and devices within the AWS system. Service teams configure the auditing features to record continuously the security-related events in accordance with requirements. The log storage system is designed to provide a highly scalable, highly available service that automatically increases capacity as the ensuing need for log storage grows. AWS Access Management procedures are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP.				

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
Authentication	DS-8.0	Enforce the use of unique usernames and passwords to access information systems.	Unique user identifiers are created as part of the onboarding workflow process in the AWS human resources management system. The device provisioning process helps ensure unique identifiers for devices. Both processes include manager approval to establish the user account or device. Initial authenticators are delivered to user's in-person and to devices as part of the provisioning process. Internal users can associate SSH public keys with their account. System account authenticators are provided to the requestor as part of the account creation process after the identity of the requestor is verified. Minimum strength of authenticators is defined by AWS including password length, requires complex passwords and password age requirements and content along with SSH key minimum bit length.	SOC 1 2.5	9.1 9.2 9.4 10.1 10.10	10.1 10.2 10.3	SI-4 AU-1 AU-2 AU-3 AU-6 AU-9 AU-11
Authentication	DS-8.1	Enforce a strong password policy for gaining access to information systems.					
Authentication	DS-8.2	Implement two-factor authentication (e.g., username/password and hard token) for remote access (e.g., VPN) to the networks.					
Authentication	DS-8.3	Implement password-protected screensavers or screen-lock software for servers and workstations.					
Authentication	DS-8.4	Consider implementing additional authentication mechanisms to provide a layered authentication strategy for WAN and LAN / Internal Network access.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			AWS Password policy and implementation is reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP.				
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)	AWS has identified auditable event categories across systems and devices within the AWS system. Service teams configure the auditing features to record continuously the security-related events in accordance with requirements. The log storage system is designed to provide a highly scalable, highly available service that automatically increases capacity as the ensuing need for log storage grows. Audit records contain a set of data elements in order to support necessary analysis requirements. In addition, audit records are available for AWS Security team or other appropriate teams to perform inspection or analysis on demand, and in response to security-related		12.4 10.4 10.1.3 10.10.3	10.1 10.2 10.3	AU-1 AU-2 AU-3 AU-6 AU-8 AU-9 AU-11 SI-4
Logging and Monitoring	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).					
Logging and Monitoring	DS-9.2	Configure logging systems to send automatic notifications when security events are detected in order to facilitate active response to incidents.					
Logging and Monitoring	DS-9.3	Investigate any unusual activity reported by the logging and reporting systems.					
Logging and Monitoring	DS-9.4a	Implement logging mechanisms on all systems used for the following: · Key generation · Key management · Vendor certificate management					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
Logging and Monitoring	DS-9.4b	Review all logs weekly, and review all critical and high daily.	or business-impacting events. Designated personnel on AWS teams receive automated alerts in the event of an audit processing failure. Audit processing failures include, for example, software/hardware errors. When alerted, on-call personnel issue a trouble ticket and track the event until it is resolved. AWS logging and monitoring processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO				
Logging and Monitoring	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)					
Logging and Monitoring	DS-9.6	Retain logs for at least one year.					
Logging and Monitoring	DS-9.7	Restrict log access to appropriate personnel.					
Mobile Security	DS-10.0	Develop a BYOD (Bring Your Own Device) policy for mobile devices accessing or storing content.	Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage mobile security devices and the access to the customer's content.		6.2 11.2		SC CA IA-2
Mobile Security	DS-10.1	Develop a list of approved applications, application stores, and application plugins/extensions for mobile devices accessing or storing content.					
Mobile Security	DS-10.2	Maintain an inventory of all mobile devices that access or store content.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
Mobile Security	DS-10.3	Require encryption either for the entire device or for areas of the device where content will be handled or stored.					
Mobile Security	DS-10.4	Prevent the circumvention of security controls.					
Mobile Security	DS-10.5	Implement a system to perform a remote wipe of a mobile device, should it be lost / stolen / compromised or otherwise necessary.					
Mobile Security	DS-10.6	Implement automatic locking of the device after 10 minutes of non-use.					
Mobile Security	DS-10.7	Manage all mobile device operating system patches and application updates.					
Mobile Security	DS-10.8	Enforce password policies.					
Mobile Security	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.	AWS provides customers the ability to use their own encryption mechanism for nearly all services including S3, EBS and EC2. VPC sessions are also encrypted. Internally, AWS establishes and manages cryptographic keys for required cryptography employed	SOC1 4.3 SOC1 4.4 SOC1 4.5 SOC1 4.6 SOC1 4.7 SOC1 4.8	8.2 10.1	3.4 3.5 3.6 4.1	IA-5 SC-8 SC-9 SC-12 SC-13
Security Techniques	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)					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
		· Drive-based encryption: (i.e., encrypting the hard drive)	within the AWS infrastructure. AWS produces, controls and distributes symmetric cryptographic keys using NIST approved key management technology and processes in the AWS information system. An AWS developed secure key and credential manager is used to create, protect and distribute symmetric keys and is used to secure and distribute: AWS credentials needed on hosts, RSA public/private keys and X.509 Certifications. AWS cryptographic processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP.				
Security Techniques	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).					
Security Techniques	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					
Security Techniques	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.					
Security Techniques	DS-11.5	Store secret and private keys (not public keys) used to encrypt					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
		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					
Security Techniques	DS-11.6	Confirm that devices on the Trusted Devices List (TDL) are appropriate based on rights owners' approval.					
Security Techniques	DS-11.7	Confirm the validity of content keys and ensure that expiration dates conform to client instructions.					
Content Tracking	DS-12.0	Implement a digital content management system to provide detailed tracking of digital content.	AWS provides customers the ability to monitor and track content within their environment, but is not responsible for the implementation and operation of these options.				
Content Tracking	DS-12.1	Retain digital content movement logs for one year.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
Content Tracking	DS-12.2	Review logs from digital content management system periodically and investigate anomalies.					
Content Tracking	DS-12.3	Use client AKAs ("aliases") when applicable in digital asset tracking systems.					
Transfer 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.	AWS provides customers the ability to use their own encryption mechanism for nearly all services including S3, EBS and EC2. VPC sessions are also encrypted. Internally, AWS establishes and manages cryptographic keys for required cryptography employed within the AWS infrastructure. AWS produces, controls and distributes symmetric cryptographic keys using NIST approved key management technology and processes in the AWS information system. An AWS developed secure key and credential manager is used to create, protect and distribute symmetric keys and is used to secure and distribute: AWS credentials needed on hosts, RSA	SOC1 4.3 SOC1 4.4 SOC1 4.5 SOC1 4.6 SOC1 4.7 SOC1 4.8	10.1 13.2	3.4 3.5 3.6 4.1	IA-5 SC-13
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.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			public/private keys and X.509 Certifications. AWS cryptographic processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP.				
Transfer Device Methodology	DS-14.0	Implement and use dedicated systems for content transfers.	AWS provides customers the ability to segment and manage networks but is not responsible for the implementation and operation of these segmented environments		12.4 13.1 13.2		AC-4 AC-20 SC-7 MP-6
Transfer Device Methodology	DS-14.1	Separate content transfer systems from administrative and production networks.					
Transfer Device Methodology	DS-14.2	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-14.4	Send automatic notifications to the production coordinator(s) upon outbound content transmission.					
Client Portal	DS-15.0	Restrict access to web portals which are used for transferring content, streaming content and key distribution to authorized users.	AWS provides customers the ability to create and manage a client portal. AWS does not implement or manage this portal on behalf of customers.		9.2 9.4 10.1 12.1 12.6 13.1 13.2		AC-2 AC-3 AC-4 AC-6 AC-20 IA-5 SC-8
Client Portal	DS-15.1	Assign unique credentials (e.g., username and password) to portal users and distribute credentials to clients securely.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
Client Portal	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).					SC-3 SI-7
Client Portal	DS-15.3	Place the web portal on a dedicated server in the DMZ and limit access to/from specific IPs and protocols.					
Client Portal	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.					
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-15.6	Do not use persistent cookies or cookies that store credentials in plaintext.					
Client Portal	DS-15.7	Set access to content on internal or external portals to expire automatically at predefined intervals, where configurable.					
Client Portal	DS-15.8	Test for web application vulnerabilities quarterly and remediate any validated issues.					
Client Portal	DS-15.9	Perform annual penetration testing of web applications and remediate any validated issues.					
Client Portal	DS-15.10	Allow only authorized personnel to request the establishment of a connection with the telecom service provider.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
Client Portal	DS-15.11	Prohibit transmission of content using email (including webmail).					
Client Portal	DS-15.12	Review access to the client web portal at least quarterly.					