AWS alignment with Motion Picture of America Association (MPAA) Content Security Best Practices – Application in the Cloud

The Motion Picture of America Association (MPAA) has established a set of best practices for Application and Cloud/Distributed Environment Security Guidelines. 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 March 17, 2015. For additional information a reference to AWS third-party audited certifications and reports is provided.

In alignment with the MPAA Best Content Security Best Practices, AWS has mapped the ISO 27002 and NIST 800-53 controls.

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
Development Lifecycle	AS-1.0	Build security into the entire Systems/Software Development Lifecycle (SDLC).	AWS applies a systematic approach to managing changes to ensure changes to customer-impacting aspects of a service are 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.	SOC1 6.1 SOC1 6.3 SOC1 6.4 SOC1 6.5 SOC1 6.6	12.5 14.1	6.1 6.2 6.3 6.4 6.5 6.6	SA-3 SA-4 SA-8 SA-11 SA-12
Development Lifecycle	AS-1.1	Test security across the entire application and infrastructure.					
Development Lifecycle	AS-1.2	Perform fuzz testing and defect remediation to discover security loopholes in software, operating systems or networks by massive inputting of random data to the system in an attempt to make it crash (e.g., buffer overflow, cross-site scripting, denial of service attacks, format bugs, SQL injection).					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
Development Lifecycle	AS-1.3	Perform bug tracking and defect remediation in conjunction with extensive black box testing, beta testing, and other proven debugging methods.					
Development Lifecycle	AS-1.4	Provide training and user guides on additions and changes to the application.					
Authentication & Access	AS-2.0	Implement secure authentication.	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	SOC1 2.1 SOC1 2.2 SOC1 2.3 SOC1 2.4 SOC1 2.5 SOC1 4.3 SOC1 4.4 SOC1 4.5 SOC1 4.6 SOC1 4.7 SOC1 4.8	9.1 9.2 9.3 9.4	7.1 8.1 8.2	AC-2 AC-3 AC-6 AC-7 AC-8 AC-14 IA-5 IA-6 IA-8
Authentication & Access	AS-2.1	Register user devices.					
Authentication & Access	AS-2.2	Implement secure password recovery.					
Authentication & Access	AS-2.3	Follow the principle of least privilege.					
Authentication & Access	AS-2.4	Implement controls to prevent brute force attacks.					
Authentication & Access	AS-2.5	Implement and document a process to secure key / cryptographic storage and ensure ongoing secure management.					
Authentication & Access	AS-2.6	Enable an auto-expiration setting to expire all external links to content after a user-defined time.					
Authentication & Access	AS-2.7	Use human verification tools such as CAPTCHA or					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
		reCAPTCHA with web applications.	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. AWS Password policy and implementation is reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP.				
Authentication & Access	AS-2.8	Provide clients with the ability to limit the number of times an asset may be downloaded or streamed by a particular user.					
Authentication & Access	AS-2.9	Confirm the upload and download of all content and critical assets.					
Authentication & Access	AS-2.10	Include a brief message on mobile applications to remind users to enable device passwords and to enable remote wipe and device location software.					
Secure Coding and Systems	AS-3.0	Perform penetration testing / web application security testing prior to production deployment, and at least quarterly thereafter. Validate vulnerabilities were remediated with a retest.	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, Boundary protection devices that employ rule sets, access control lists (ACL), and configurations enforce the flow of information between	SOC1 3.4 SOC1 3.6 SOC1 10.4	8.1 8.2 8.3 10.1 12.2 12.6 13.1 13.2	1.2 1.3 1.4 5.1 5.2 5.3 10.6 11.1 11.2 11.3	AC-18 AU-5 CA-3 CA-9 SC-15 SC-18 SC-19 SC-32 SC-7 SI-10 SI-11 SI-2 SI-3
Secure Coding and Systems	AS-3.1	Perform vulnerability testing at least quarterly.					
Secure Coding and Systems	AS-3.2	Utilize cookies in a secure manner, if they need to be used					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
Secure Coding and Systems	AS-3.3	Validate user input and implement secure error handling.	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 network fabrics restrict the flow of information to specific information system services. Access control lists and rule sets are reviewed and approved, and are				SI-4 SI-8
Secure Coding and Systems	AS-3.4	Implement secure logging procedures.					
Secure Coding and Systems	AS-3.5	Implement an SIEM (Security Information Event Management System) to aggregate and analyze the disparate logs.					
Secure Coding and Systems	AS-3.6	Encrypt all content and client data at rest.					
Secure Coding and Systems	AS-3.7	Encrypt all content and client data in transit.					
Secure Coding and Systems	AS-3.8	Implement controls for secure session management.					
Secure Coding and Systems	AS-3.9	Implement controls to prevent SQL injection.					
Secure Coding and Systems	AS-3.10	Implement controls to prevent unvalidated URL redirects and forwards.					
Secure Coding and Systems	AS-3.11	Implement controls to prevent connections from anonymity networks (e.g., Tor, Freenet, Netshade), if possible.					
Secure Coding and Systems	AS-3.12	Implement controls to prevent IP address leakage.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
Secure Coding and Systems	AS-3.13	Implement controls to prevent XSS (Cross-site scripting).	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 scanning is performed and any unnecessary ports or protocols in use are corrected.				
Secure Coding and Systems	AS-3.14	Allow senders the option to include session-based forensic (invisible) watermarking for content.					
Secure Coding and Systems	AS-3.15	Implement a formal, documented content / asset lifecycle.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			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.				
Organization & Management	CS-1.0	Compliance with the MPAA Content Best Practices Common Guidelines is required. Where stronger controls exist within the Application Security and Cloud/Distributed Environment Guidelines, the stronger policy will prevail.	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 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,	SOC1 1.1 SOC1 1.2 SOC2 9.3 SOC2 9.4 SOC2 9.8 SOC2 10.1 SOC2 10.3 SOC2 10.4	5.1 6.1	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	AC-1 AC-18 AC-19 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IR-1 MA-1 MP-1 PE-1 PL-1 PS-1 RA-1
Organization & Management	CS-1.1	Perform a third party security audit at least once per year (e.g., SSAE 16 Type 2, SOC 1, ISO 27000/27001, MPAA).					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
Organization & Management	CS-1.2	Document and implement security and privacy policies that are aligned with security industry frameworks for Information Security Management (e.g., ISO-27001, ISO-22307, CoBIT).	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 operates 24x7x365 coverage to detect incidents and manage the impact to resolution. AWS roles & Responsibilities are reviewed by			12.3 12.4	SC-1 SI-1
Organization & Management	CS-1.3	Document and implement information security baselines for every component of the infrastructure (e.g., Hypervisors, operating systems, routers, DNS servers, etc.).					
Organization & Management	CS-1.4	Document and implement personnel security procedures that align with the organization's current information security procedures.					
Organization & Management	CS-1.5	Require all employees, contractors, and third parties to sign confidentiality / non-disclosure agreements when going through the onboarding process.					
Organization & Management	CS-1.6	Document and implement procedures for conducting security due diligence					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
		when offloading functionality or services to a third party.	independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance				
Organization & Management	CS-1.7	Document and implement segregation of duties for business critical tasks.					
Organization & Management	CS-1.8	Provide clients with information regarding locations for their content and data.					
Organization & Management	CS-1.9	Develop a documented procedure for responding to requests for client data from governments or third parties.					
Organization & Management	CS-1.10	Establish policies and procedures for labeling, handling, and securing containers that contain data and other containers.					
Organization & Management	CS-1.11	Establish procedures for the secure deletion of content/data, including archived and backed-up content/data.					
Organization & Management	CS-1.12	Establish, document and implement scenarios to clients in which client content/data may be moved from one physical location to another.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
Organization & Management	CS-1.13	Establish, document and implement additional key management features, controls, policies and procedures.					
Organization & Management	CS-1.14	Train personnel regarding all policies and procedures.					
Organization & Management	CS-1.15	Establish a process to notify clients when material changes are made to security/privacy policies.					
Organization & Management	CS-1.16	Plan, prepare and measure the required system performance to ensure acceptable service levels.					
Organization & Management	CS-1.17	Develop and maintain additional requirements for incident response and immediate notification to the client in the event of any unauthorized access to systems or content.					
Operations	CS-2.0	Secure datacenter utilities services and environmental conditions.	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	SOC1 5.1 SOC1 5.3 SOC1 5.4 SOC1 5.5 SOC1 5.6 SOC1 5.7 SOC1 5.8 SOC1 5.9	11.1 11.2 11.5	1.1 1.5 2.5 3.1 3.7 4.3 5.4 6.7	PE-1 PE-18 PE-2 PE-3 PE-4 PE-5 PE-6 PE-8
Operations	CS-2.1	Ensure the data center has appropriate perimeter and physical security controls.					
Operations	CS-2.2	Develop, document and maintain additional					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
		requirements for business continuity planning.	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 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	SOC1 5.10 SOC1 5.11 SOC1 5.12 SOC1 10.4		7.3 8.1 8.4 8.8 9.2 9.4 9.10 10.8 11.6 12.1 12.3	PE-9 PL-8 PS-1
Operations	CS-2.3	Develop, document and maintain additional change and configuration controls.					
Operations	CS-2.4	Maintain a complete inventory of all critical assets, including ownership of the asset.					
Operations	CS-2.5	Maintain an inventory of all critical supplier relationships.					
Operations	CS-2.6	Develop and maintain service level agreements (SLA's) with clients, partners, and service providers.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
			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.				
Data Security	CS-3.0	Implement a process to provide all relevant logs requested for good cause to clients in a format that can be easily exported from the platform for analysis in the event of a security incident.	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 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	SOC1 3.1 SOC1 3.2 SOC1 3.3 SOC1 3.5 SOC1 3.6 SOC1 3.9 SOC1 3.10 SOC1 3.11 SOC1 3.12 SOC1 3.13 SOC1 3.14 SOC1 3.15 SOC1 3.16 SOC1 7.1 SOC1 7.2 SOC1 7.3 SOC1 7.4 SOC1 7.5 SOC1 7.6 SOC1 7.7 SOC1 7.8 SOC1 10.4	11.2 12.1	1.1 1.2 1.3 1.4 6.4 10.4 12.5	AC-3 AC-4 AC-5 AU-8 CA-3 CA-9 CM-6 CM-7 SC-19 SC-5 SC-7 SI-4
Data Security	CS-3.1	Consider providing the capability to use system geographic location as an additional authentication factor.					
Data Security	CS-3.2	Provide the capability to control the physical location/geography of storage of a client's content/data, if requested.					
Data Security	CS-3.3	Establish procedures to ensure that non-production data must not be replicated to production environments.					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
Data Security	CS-3.4	Establish, document and implement a published procedure for exiting the service arrangement with a client, including assurance to sanitize all computing systems of client content/data once the client contract has terminated.	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 with SOC, PCI DSS, ISO 27001 and FedRAMP.				
Data Security	CS-3.5	Establish and document policies and procedures for secure disposal of equipment, categorized by asset type, used outside the organization's premises.					
Data Security	CS-3.6	Implement a synchronized time service protocol (e.g., NTP) to ensure all systems have a common time reference.					
Data Security	CS-3.7	Design and configure network and virtual environments to restrict and monitor traffic between trusted and untrusted connections.					
Data Security	CS-3.8	Design, develop and deploy multi-tenant applications, systems, and components such that					

Security Topic	No.	Best Practice	AWS Implementation	AWS SOC	ISO 27002	AWS PCI v.3.1	NIST 800-53 Rev4
		client content and data is appropriately segmented.					
Data Security	CS-3.9	Use secure and encrypted communication channels when migrating physical servers, applications, and content data to/from virtual servers.					
Data Security	CS-3.10	Implement technical measures and apply defense-in-depth techniques (e.g., deep-packet analysis, traffic throttling, black-holing) for detection and timely response to network-based attacks associated with unusual ingress/egress traffic patterns (e.g., NAC spoofing and ARP poisoning attacks and/or DDOS attacks).					
Data Security	CS-3.11	Establish and document controls to secure virtualized environments.					