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.fightlimtheft.org/best-practice.html

The table below was created by AWS to highlight the deta between the MPAA best practices published in 2013 and the MPAA best practices published in 2015. • For any new control added to the 2015 MPAA best practices, see any rows highlighted in "green." • For any control set which had a sight change between the 2013 MPAA best practices, and the 2015 best practices, see any row highlighted in "blue." • For any control set which had a sight the requirements behad the controls were highlighted in "greyn." • Any control set which is not highlighted the requirements the hold the controls were highlighted in "blue."

	No. MS-1.0	Best Practice Establish an information security management system that implements	Security Topic	No. MS.S-1.0	Best Practice Establish an information security management system that implements	The difference with the 2015 standard is the requirement for policies
	MS-1.0	a control framework for information security which is approved by the		MS.S-1.0	a control framework (e.g., ISO 27001) for information security which is	The difference with the 2015 standard is the requirement for policies and processes to be reviewed at least annually vs. periodically
		business owner(s) /senior management.			approved by executive management/owner(s)	
Executive Security Awareness/ Oversight	MS-1.1	Review information security management policies and processes at least annually.	Executive Security Awareness / Oversight	MS-1.1	Train and engage executive management/owner(s) on the business' responsibilities to protect content	
Executive Security Awareness/ Oversight	MS-1.2	Train and engage executive management/owner(s) on the business'	Executive security Awareness / Oversight	MS-1.0	Ensure executive management/owner(s) oversight of the Information	
		responsibilities to protect content at least annually.			Security function by requiring periodic review of the information security program and risk assessment results	
	MS-1.3	Create an information security management group to establish and review information security management policies.				
	MS-2.0	Develop a formal, documented security risk assessment process focused		MS-2.1	Identify high-security content based on client instruction	The difference with the 2015 standard is the requirement for a
		on content workflows and sensitive assets in order to identify and prioritize risks of content theft and leakage that are relevant to the				formalized risk assessment process vs. based on client instruction.
Risk Management	MS-2.1	facility. Conduct an internal risk assessment annually and upon key workflow	Risk Management	MS-2.2	Conduct an internal risk assessment annually and upon key workflow	
		changes-based on, at a minimum, the MPAA Best Practice Common			changes-based on, at a minimum, the MPAA Best Practice Common	
		Guidelines and the applicable Supplemental Guidelines—and document and act upon identified risks.			Guidelines and the applicable Supplemental Guidelines—and document and act upon identified risks	
	MS-3.0	Identify security key point(s) of contact and formally define roles and responsibilities for content and asset protection.		MS-3.0	Identify security key point(s) of contact and formally define roles and responsibilities for content and asset protection	With the 2015 standard, the requirement for establishing a security team was removed.
Security Organization			Security Organization	MS.S-3.0	Establish a security team that is responsible for proactively monitoring information systems and physical security to identify and respond to any	
					suspicious activity	
	MS-4.0	Establish policies and procedures regarding asset and content security; policies should address the following topics, at a minimum:		MS-4.0	Establish policies and procedures regarding asset and content security; policies should address the following topics, at a minimum:	With the 2015 standard, the requirement for a human resource polic and client asset removal - were removed. The requirement for polici
		 Acceptable use (e.g., social networking, Internet, phone, personal devices, mobile devices, etc.) 			Human resources policies Acceptable use (e.g., social networking, Internet, phone, etc.)	around business continuity, confidentiality, incident response, mobil device, network: internet and wireless, security policy, visitor policy,
		 Asset and content classification and handling policies 			Asset classification	disciplinary - were added.
		Business continuity (backup, retention and restoration) Change control and configuration management policy			Asset handling policies Digital recording devices (e.g., smart phones, digital cameras,	
		Confidentiality policy Digital recording devices (e.g., smart phones, digital cameras,			camcorders) • Exception policy (e.g., process to document policy deviations)	
		camcorders)			 Password controls (e.g., password minimum length, screensavers) 	
		Exception policy (e.g., process to document policy deviations) Incident response policy			Prohibition of client asset removal from the facility System change management	
		Mobile device policy Network, internet and wireless policies			Whistleblower policy Sanction policy (e.g., disciplinary policy)	
		 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)				
	MS-4.1	Review and update security policies and procedures at least annually.		MS.S-4.0	Provide in-depth training specific to the content handled by the facility	
	MS-4.2	Communicate and require sign-off from all company personnel (e.g.,		MS-4.1	Review and update security policies and procedures at least annually	
		employees, temporary workers, interns) and third party workers (e.g., contractors, freelancers, temp agencies) for all current policies,				
Policies and Procedures	MS-4.3	procedures, and/or client requirements. Develop and regularly update an awareness program about security	Policies and Procedures	MS.S-4.1	Provide training on the applications and processes surrounding	
		policies and procedures and train company personnel and third party workers upon hire and annually thereafter on those security policies and			encryption and key management for all individuals who handle encrypted content	
		procedures, addressing the following areas at a minimum:			entrypted content	
		IT security policies and procedures Content/asset security and handling in general and client-specific				
		requirements • Security incident reporting and escalation				
		Disciplinary policy				
		 Encryption and key management for all individuals who handle encrypted content 				
		Asset disposal and destruction processes				
				MS-4.2	Require a sign-off from all company personnel (e.g., employees,	
					temporary workers, interns) and third party workers (e.g., contractors, freelancers, temp agencies) for all policies, procedures, and/or client	
					requirements and any updates	
				MS-4.3	Develop and regularly update a security awareness program and train	
					company personnel and third party workers upon hire and annually	
					thereafter on the security policies and procedures, addressing the	
					following areas at a minimum:	
					following areas at a minimum: • IT security policies and procedures • Content/asset security and handling	
					following areas at a minimum: • IT security policies and procedures	
	MS-5.0	Establish a formal incident response plan that describes actions to be		MS-5.0	following areas at a minimum: • IT security policies and procedures • Content/asset security and handling • Security incident reporting and escalation	The control requirements behind the control set did not change
		taken when a security incident is detected and reported.			following areas at a minimum: 1 T ecurity policies and procedures • Content/Asset security and handling • Security incident reporting and escalation • Disciplinary measures Establish a formal incident response plan that describes actions to be taken when a security incident tis detected and reported	The control requirements behind the control set did not change between 2015 and 2013.
	MS-5.0 MS-5.1			MS-5.0 MS-5.1	following areas at a minimum: 11 Security policies and procedures • Content/asset security and handling • Security in clident reporting and escalation • Disciplinary measures Establish a formal incident response plan that describes actions to be	
		taken when a security incident is detected and reported. Identify the security incident response team who will be responsible for	heiden		following areas at a minimum: 11 Security policies and procedures • Content/Lisses security and handling • Security incident reporting and escalation • Disciplinary measures Establish a formal incident response plan that describes actions to be taken when a security incident is detected and reported identify the security incident is detected and perported	
Incident Response	MS-5.1	taken when a security incident is detected and reported. Identify the security incident response team who will be responsible for detecting, analyzing, and remediating security incidents.	Incident Response	MS-5.1	following areas at a minimum: 11 Security policies and procedures • Content/Jasset security and handling • Society invident reporting and escalation • Society measures Establish a formal incident response plan that describes actions to be taken when a security incident is detected and reported Identify the security incident is detected and peopred detecting, analyzing, and remediating security incidents	
Incident Response	MS-5.1	taken when a security incident is detected and reported. identify the security incident reported area who will be responsible for detecting, analysing, and remediating security incidents. Establish a security incident reporting process for individuals to report detected incidents to be security incident response team. Communicate incidents promptly to clients whose content may have	Incident Response	MS-5.1	following areas at a minimum: 1 of security policies and procedures • Content/Assets security and handling • Societary incident reporting and escalation • Disciplinary measures Establish a formal incident response plan that describes actions to be tableting a formal incident response plan that describes actions to be tableting a formal incident response taum show all be responsible for detecting, analyzing, and remediating security incidents stabilities ascurity incident response taum for walls and to report detected incidents promptly to clients whose content may have	
Incident Response	MS-5.1 MS-5.2	taken when a security incident is detected and reported. tionity the security incident reported area who will be responsible for detecting, analysing, and remediating security incidents. Establish a security incident reporting process for individuals to report detected incidents to the security incident response team. Communicate incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client seets), and conduct a post-mortem meeting with management and	Incident Response	MS-5.1 MS-5.2	following areas at a minimum: 1 of security policies and procedures • Content/Asset security and handling • Security incident reporting and escalation • Disciplinary measures Establish a formal incident response plan that describes actions to be taken when a security incident is detected and reported identify the security incident response team who will be responsible for detecting analysing and remediating security incident security incident resportse process for individuals to report detected incidents to the security incident response team Communicate incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client sets), and conduct a post-morter meeting with management and	
Incident Response	MS-5.1 MS-5.2 MS-5.3	taken when a security incident is detected and reported. isonity the security incident response team who will be responsible for detecting, analyzing, and remediating security incidents. Establish a security incident reporting process for individuals to report. detected incidents to the security incident response team. Communicate incidents promptly to clients whose content may have been leaked, store or otherwise composite (e.g., missing client assets), and conduct a post-mortem meeting with management and client.	Incident Response	MS-5.1 MS-5.2	following areas at a minimum: 1 of excurity policies and procedures 4 - Content/Asset security and handling 5 - Security incident reporting and escalation 4 - Disciplinary measures Establish a formal incident response plan that describes actions to be tidentify the security incident tidetected and reported lidentify the security incident response team who will be responsible for detecting, analyzing, and remediating security incidents Establish a security incident response steam who will be responsible for detecting, analyzing, and remediating security incident Establish as ecurity incident response team who been leaked, store or otherwise componies (e.g., missing client	between 2015 and 2013.
Incident Response Business Continuity & Disaster Recovery	MS-5.1 MS-5.2 MS-5.3 MS-6.0	taken when a security incident is detected and reported. tentify the security incident response team who will be responsible for detecting, analyzing, and remediating security incidents. Establish a security incident response team. Communicate incidents to the security incident response team. Communicate incidents to the security incident response team. Communicate incidents promptly to client whose content may have been leaked, stored or otherwise compromised (e.g., missing Clent assets), and conduct a post-mortern meeting with management and client. Establish formal plan that describes actions to be taken to ensure business continuty.	Incident Response	MS-5.1 MS-5.2	following areas at a minimum: 1 of security policies and procedures • Content/Asset security and handling • Security incident reporting and escalation • Disciplinary measures Establish a formal incident response plan that describes actions to be taken when a security incident is detected and reported identify the security incident response team who will be responsible for detecting analysing and remediating security incident security incident resportse process for individuals to report detected incidents to the security incident response team Communicate incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client sets), and conduct a post-morter meeting with management and	
	MS-5.1 MS-5.2 MS-5.3 MS-6.0 MS-6.1	taken when a security incident is detected and reported. Identify the security incident response team who will be responsible for detecting, analysing, and remediating security incidents. Establish a security incident reporting process for individuals to report detected incidents to the security incident response team. Communicate incidents promptly to clients whose content may have been leaded, stoller or otherwise compromade (e.g., missing Client detected incidents poromethy to clients whose content may have been leaded, stoller or otherwise compromade (e.g., missing Client detected incidents poromethy incidentes with management and during. Establish a formal plan that describes actions to be taken to ensure business continuity.	Incident Response	MS-5.1 MS-5.2	following areas at a minimum: 1 of security policies and procedures • Content/Asset security and handling • Security incident reporting and escalation • Disciplinary measures Establish a formal incident response plan that describes actions to be taken when a security incident is detected and reported identify the security incident response team who will be responsible for detecting analysing and remediating security incident security incident resportse process for individuals to report detected incidents to the security incident response team Communicate incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client sets), and conduct a post-morter meeting with management and	between 2015 and 2013. 2015 MPAA added this control set.
Business Continuity & Disaster Recovery Change Control & Configuration	MS-5.1 MS-5.2 MS-5.3 MS-6.0	taken when a security incident is detected and reported. Identify the security incident reported area who will be responsible for detecting, analysing, and remediating security incidents. Establish a security incident reporting process for individuals to report detected incidents to the security incident response team. Communicate incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client asset), and conduct a post-mortem meeting with management and client. Establish a formal plan that describes actions to be taken to ensure business continuity.	Incident Response	MS-5.1 MS-5.2	following areas at a minimum: 1 of security policies and procedures • Content/Asset security and handling • Security incident reporting and escalation • Disciplinary measures Establish a formal incident response plan that describes actions to be taken when a security incident is detected and reported identify the security incident response team who will be responsible for detecting, analysing, and remediating security incident security incident resportse grocess for individuals to report detected incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client aset), and conduct a post-mortem growthered and the security incident response team the security incident	between 2015 and 2013.
Business Continuity & Disaster Recovery	MS-5.1 MS-5.2 MS-5.3 MS-6.0 MS-6.1 MS-7.0	taken when a security incident is detected and reported. Identify the security incident response team who will be responsible for detecting, analysing, and remediating security incidents. Stabilish ascurity incident reporting process for individuals to report detected incidents to the security incident response team. Communicate incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client sates), and conduct a post-mortem meeting with management and client. Exabilish a forman Jpan that describes actions to be taken to ensure business continuity. Meeting and remediating continuity incidents. Exabilish policies and procedures to ensure new data, applications, network, and systems components have been pre-approved by business	Incident Response	MS-5.1 MS-5.2 MS-5.3	following areas at a minimum: 1 of security policies and procedures 4 - Content/Asset security and handling 5 - Content/Asset security and handling 5 - Execurity incident response plan that describes actions to be taken when a security incident response plan that describes actions to be taken when a security incident response team who will be responsible for directing, analysing, and remediating security incidents Establish a recurity incident response team who will be responsible for detecting, analysing, and remediating security incidents Establish a security incident response process for individuals to report detected incidents to the security incident response team Communicate incidents prompti to clicks whose content may have been leaked, stolen or otherwise compromised (e.g., missing client asset), and conduct a post-mortem meeting with management and client	between 2015 and 2013. 2015 MPAA added this control set. 2015 MPAA added this control set.
Business Continuity & Disaster Recovery Change Control & Configuration	MS-5.1 MS-5.2 MS-5.3 MS-6.0 MS-6.1	taken when a security incident is detected and reported. Identify the security incident reported area who will be responsible for detecting, analysing, and remediating security incidents. Stabilish ascurity incident reporting process for individuals to report detected incidents to the security incident response team. Communicate incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client sates), and conduct a post-mortem meeting with management and client. Establish a forman Jpan that describes actions to be taken to ensure business continuity. Mentify the business continuity incidents. Establish policies and procedures to ensure new data, applications, network, and systems components have been pre-approved by business ladership. Document workflows tracking content and authorization checkpoints.	Incident Response	MS-5.1 MS-5.2	following areas at a minimum: 1 of security pidders and procedures • Content/Asset security and handling • Security hidden reporting an escalation • Disciplinary measures Establish a formal incident response plan that describes actions to be taken when a security incident tis detected and reported identify the security incident response team who will be responsible for detecting, analysing, and remediating security incident tis detecting establish a security incident reporting process for individuals to report detecting analysing, and remediating security incident response team Communicate hickens promptly to clients whose content may have been leaked, stolen or otherwise compromised for g, missing client assets), and conduct a post-mortem meeting with management and client Document a workflow that includes the tracking of content and authorization checkpoints throughout each process, include the	between 2015 and 2013. 2015 MPAA added this control set.
Business Continuity & Disaster Recovery Change Control & Configuration	MS-5.1 MS-5.2 MS-5.3 MS-6.0 MS-6.1 MS-7.0	taken when a security incident is detected and reported. Identify the security incident reported area who will be responsible for detecting, analyzing, and remediating security incidents. Establish a security incident reporting process for individuals to report detected incidents to the security incident response team. Communicate incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client sates), and conduct a post-mortem meeting with management and client. Establish a formar Jpan that describes actions to be taken to ensure business continuity. Biotenty the business continuity incidents. Establish policies and procedures to source new data, applications, network, and systems components have been pre-approved by business adventity. Document workflows tracking content and authorization checkpoints. Include the following processes for both physical and digital content: • Delivery (necelpt/return)	Incident Response	MS-5.1 MS-5.2 MS-5.3	following areas at a minimum: I of security holders and procedures • Content/Asset security and handling • Security holders reporting and escalation • Disciplinary measures Establish a formal incident response plan that describes actions to be taken when a security incident is detected and reported identify the security incident response team who will be responsible for detecting, analysing, and remediating security incident is detecting establish a security incident response team who will be responsible for detecting, analysing, and remediating security incident response team Communicate holders grouphy to detect response team Communicate holders grouphy to detect whose content may have been leaked, stolen or otherwise compromised for g., missing dient averk1, and conduct a post-mortem meeting with management and client Document a workflow that includes the tracking of content and authorization checkpoints throughout each process, include the following processes for both physical and digital content: • Delivery	between 2015 and 2013. 2015 MPAA added this control set. 2015 MPAA added this control set. The control requirements behind the control set did not change
Business Continuity & Disaster Recovery Change Control & Configuration	MS-5.1 MS-5.2 MS-5.3 MS-6.0 MS-6.1 MS-7.0	taken when a security incident is detected and reported. (dentify the security incident reporte and who will be responsible for detecting, analysing, and mendiating security incidents. Establish a security incident reporting process for individuals to report detected incidents to be security incident response team. Communicate incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing Client stols), and conduct a post-mortem menticity with management and client detecting, and provident to approximate the security incidents. Establish policies, and procedures to ensure med wata, applications, relativity, and systems components have been pre-approved by business leadership. Document workflows tracking content and authorization chickspoints. Include the following processs for both physical and digital content: Beiney (receipter eturn)	Incident Response	MS-5.1 MS-5.2 MS-5.3	following areas at a minimum: I of security holden is and procedures • Content/Assets security and handling • Sontent/Assets security and handling • Society holden terporting and escalation • Disciplinary measures Edablina formal incident response plan that describes actions to be taken where a security incident to detected and reported tentfly the security incident response taw show allo be responsible for detecting, analyzing, and remediating security incidents Establish a security incident response taw show allo be responsible for detecting, analyzing, and remediating security incidents Establish a security incident response taw show allo be responsible for detected incidents to the security incident response team 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 Document a workflow that includes the tracking of content and authorization checkpoints throughout each process, include the following processes for both physical and digital content:	between 2015 and 2013. 2015 MPAA added this control set. 2015 MPAA added this control set. The control requirements behind the control set did not change
Business Continuity & Disaster Recovery Change Control & Configuration	MS-5.1 MS-5.2 MS-5.3 MS-6.0 MS-6.1 MS-7.0	taken when a security incident is detected and reported. identify the security incident reporte area who will be responsible for detecting, analysing, and remediating security incidents. Establish a security incident reporting process for individuals to report detected incidents to the security incident response team. Communicate incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client sates); and conduct a post-mortem meeting with management and client. Establish a formal plan that describes actions to be taken to ensure builty the builty same of the meeting with management and client. Establish policies, and procedures to ensure new data, applications, metwork, and systems components have been pre-approved by business leaderablus. Document workflows tracking content and authorization checkspoints. Include the following processes for both physical and digital content: • Belwey (necespt/return) • Ingest	Incident Response	MS-5.1 MS-5.2 MS-5.3	following areas at a minimum: I off security piddes and procedures • Content/Asset security and handling • Security incident reporting and esclation • Disciplinary measures Establish a formal incident response plan that describes actions to be taken when a security incident is detected and reported identify the security incident response team who will be responsible for detecting, analysing, and remediating security incident testablish a security incident response team who will be response be communicate incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client asset), and conduct a post-mortem meeting with management and client Discument a workflow that includes the tracking of content and authorization checkpoints throughout each process include the following processes for both physical and digital content: • Dievery • Movement • Storage	between 2015 and 2013. 2015 MPAA added this control set. 2015 MPAA added this control set. The control nequirements behind the control set did not change
Business Continuity & Disaster Recovery Change Control & Configuration Management	MS-5.1 MS-5.2 MS-5.3 MS-6.0 MS-6.1 MS-7.0	taken when a security incident is detected and reported. Identify the security incident response team who will be responsible for detecting, analysing, and remediating security incidents. Stabilish a security incident response team. Communicate incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client sates), and conduct a post-mortem weeting with management and client. Stabilish a formal plan that describes actions to be taken to ensure business contraulity. Establish a procedures to serve may have been pre-approved by business direttly the business continuity incidents. Estabilish policies and procedures to ensure new data, applications, network, and systems components have been pre-approved by business detecting, making processes for both physical and digital contents: to Leiberry (necel/r/teum) Bingest * Movement * Storage		MS-5.1 MS-5.2 MS-5.3	following areas at a minimum: I of security piddles and procedures • Content/Asset security and handling • Security incident reporting and escalation • Disciplinary measures Establish a formal incident response plan that describes actions to be taken when a security incident is detected and reported identify the security incident response team who will be responsible for detecting, analysing, and remediating security incident establish a security incident response team who will be response be for detecting, analysing, and remediating security incident establish a security incident response team for an experiment detected incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client asset), and conduct a post-morter meeting with management and client Discomment a workflow that includes the tracking of content and anthoritation indexposits for both physical and digital content: • Dislawing Noncement • Storage • Removal from the site	between 2015 and 2013. 2015 MPAA added this control set. 2015 MPAA added this control set. The control nequirements behind the control set did not change
Business Continuity & Disaster Recovery Change Control & Configuration Management	MS-5.1 MS-5.2 MS-6.0 MS-6.0 MS-6.1 MS-7.0 MS-8.0	taken when a security incident is detected and reported. identify the security incident reported area who will be responsible for detecting, analysing, and remediating security incidents. Establish a security incident reporting process for individuals to report detected incidents to be security incident response team. Communicate incidents promotily to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client asset), and conduct a post-mortem meeting with management and client. Establish formal plan that describes actions to be taken to ensure business continuity. Establish policies and procedures to serve new data, applications, network, and systems components have been pre-approved by business indentify the business continuity individents. Establish policies and procedures to serve new data, applications, network, and systems components have been pre-approved by business indentify the business containing content and authorization checkpoints. Thouse the following processes for both physical and digital content: • Server (receipt/return) • Wore ment: • Wore ment: • Removal/destruction		MS-5.1 MS-5.2 MS-5.3 MS-6.0	following areas at a minimum: I of security piddles and procedures • Content/Asset security and handling • Security incident reporting and escalation • Disciplinary measures Establish a formal incident response plan that describes actions to be taken when a security incident is detected and reported identify the security incident response team who will be responsible for detecting analysing, and remediating security incident security incident response team who will be response be for detecting analysing, and remediating security incident stabilith a security incident response team for any detected incidents to the security incident response team Communicate incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client assets), and conduct a post-morter meeting with management and client Document a workflow that includes the tracking of content and anthomation checkpoints throughout each process, include the following processes for both physical and digital content: • Movement • Storement • Storement • Storement • Storement • Discussion • Remoul from the gite • Destruction	between 2015 and 2013. 2015 MPAA added this control set. 2015 MPAA added this control set. The control nequirements behind the control set did not change
Business Continuity & Disaster Recovery Change Control & Configuration Management	MS-5.1 MS-5.2 MS-5.3 MS-6.0 MS-6.1 MS-7.0	taken when a security incident is detected and reported. Identify the security incident response team who will be responsible for detecting, analysing, and remediating security incidents. Establish ascurity incident reporting process for individuals to report detected incidents to the security incident response team. Communicate incidents promptly to clients whose content may have been isked, stolen or otherwise compromade (e.g., missing Client stolents). Communicate incidents promptly to clients whose content may have been isked, stolen or otherwise compromade (e.g., missing Client stolents). Communicate incidents promptly to clients whose content may have been isked, stolen or otherwise compromede (e.g., missing Client stolents). Catablish a formal plan that describes actions to be taken to ensure business continuity. Stablish policies and procedures to ensure new data, applications, include the business components have been pre-approved by business leaderchip. Document vonkflows tracking content and authorization checkpoints. Include the following processes for both physical and digital content: • Johney (recell/return) • Johney • Johney (destruction Update the workflow when there are changes to the process, and review		MS-5.1 MS-5.2 MS-5.3	following areas at a minimum: I of security piddles and procedures • Content/Asset security and handling • Security incident reporting and escalation • Disciplinary measures Establish a formal incident response plan that describes actions to be taken when a security incident is detected and reported identify the security incident response team who will be responsible for detecting, analysing, and remediating security incident establish a security incident response team who will be response be for detecting, analysing, and remediating security incident establish a security incident response team for an experiment detected incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client asset), and conduct a post-morter meeting with management and client Discomment a workflow that includes the tracking of content and anthoritation indexposits for both physical and digital content: • Dislawing Noncement • Storage • Removal from the site	between 2015 and 2013. 2015 MPAA added this control set. 2015 MPAA added this control set. 2015 MPAA added this control set.
Business Continuity & Disaster Recovery Change Control & Configuration Management	MS-5.1 MS-5.2 MS-5.3 MS-6.0 MS-6.0 MS-6.1 MS-7.0 MS-8.0	taken when a security incident is detected and reported. identify the security incident reporte and who will be responsible for detecting, analysing, and remediating security incidents. Establish a security incident reporting process for individuals to report detected incidents to the security incident response team. Communicate incidents promptly to clients whose content may have been isaked, stolen or otherwise compromised (e.g., missing Client stoles), and conduct a post-mortem meeting with management and translands. A formal plant that describes actions to be taken to ensure business continuity: density the business continuity incidents. Establish policies and procedures to ensure new data, applications, relevork, and systems components have been pre-approved by business ladereding). Document workflows tracking content and authorization checkpoints. Include the following processes for both physical and digital content: • a longe • a longet • a longet • a longet • a longet • a longet Update the workflow when there are changes to the process, and review the workflow process at least annually to identify changes.		MS-5.1 MS-5.2 MS-5.3 MS-6.0	following areas at a minimum: I of security holden is and procedures • Content/Asset security and handling • Sontent/Asset security and handling • Societary incident response gain that describes actions to be taken where a security incident tagence tau who will be responsible for detecting, analyzing, and remediating security incidents Establish a neurity incident response tau who will be responsible for detecting, analyzing, and remediating security incidents Establish a security incident response tau who will be responsible for detecting, analyzing, and remediating security incidents Establish a security incident response tau who will be responsible for detected incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client assets), and conduct a post-morem meeting with management and client Document a workflow that includes the tracking of content and authorization checkpoints throughout each process, include the following processes for both physical and digital content: • Delivery • Ingest • Movement • Storage • Destruction • Responsed from the size • Destruction	between 2015 and 2013. 2015 MPAA added this control set. 2015 MPAA added this control set. The control nequirements behind the control set did not change between 2015 and 2013.
Business Continuity & Disaster Recovery Change Control & Configuration Management	MS-5.1 MS-5.2 MS-6.0 MS-6.0 MS-6.1 MS-7.0 MS-8.0	taken when a security incident is detected and reported. Identify the security incident response team who will be responsible for detecting, analysing, and remediating security incidents. Establish ascurity incident reporting process for individuals to report detected incidents to the security incident response team. Communicate incidents promptly to clients whose content may have been isked, stolen or otherwise compromade (e.g., missing Client stolents). Communicate incidents promptly to clients whose content may have been isked, stolen or otherwise compromade (e.g., missing Client stolents). Communicate incidents promptly to clients whose content may have been isked, stolen or otherwise compromede (e.g., missing Client stolents). Catablish a formal plan that describes actions to be taken to ensure business continuity. Stablish policies and procedures to ensure new data, applications, include the business components have been pre-approved by business leaderchip. Document vonkflows tracking content and authorization checkpoints. Include the following processes for both physical and digital content: • Johney (recell/return) • Johney • Johney (destruction Update the workflow when there are changes to the process, and review		MS-5.1 MS-5.2 MS-5.3 MS-6.0	following areas at a minimum: I of security holden is and procedures • Content/Asset security and handling • Sontent/Asset security and handling • Sontent/Asset security and handling • Social with a security incident separate tawn show allo exponsible for detecting, analyzing, and remediating security incidents Establish a security incident response tawn show allo eresponsible for detecting, analyzing, and remediating security incidents Establish a security incident response tawn show allo eresponsible for detecting, analyzing, and remediating security incidents Establish a security incident response tawn show allo eresponse the detected 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 Document a workflow that includes the tracking of content and authorization checkpoints throughout each process, include the following processes for both physical and digital content: • Delivery • Ingest • Movement • Arrouged from the size • Destruction turnet, implement, and assess the effectiveness of key controls to Destruction	between 2015 and 2013. 2015 MPAA added this control set. 2015 MPAA added this control set. The control nequirements behind the control set did not change
Business Continuity & Disaster Recovery Change Control & Configuration Management Workflow Segregation of Duties	MS-5.1 MS-5.2 MS-5.3 MS-6.0 MS-6.1 MS-6.0 MS-8.1 MS-8.1	taken when a security incident is detected and reported. Identify the security incident reported area who will be responsible for detecting, analysing, and remediating security incidents. Establish a security incident reporting process for individuals to report detected incidents to be security incident response team. Communicate incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client asset), and conduct a post-mortem meeting with management and client. Establish formal plan that describes actions to be taken to ensure business continuity. Identify the business continuity incidents. Establish policies and procedures to serve new data, applications, network, and systems components have been pre-approved by business identify the business continuity incidents. Establish policies and procedures to serve new data, applications, network, and systems components have been pre-approved by business identify the business continuity incidents. Establish policies and procedures to serve new data, applications, network, and systems components have been pre-approved by business identify the business continuity incidents. Establish policies and procedures to serve new data, applications, network, and systems components have been pre-approved by business identify the business components have been pre-approved by business identify the business to be business in a digital content: • enlewy (receipt/return) • update the workflow when there are changes to the process, and review the workflow process at least annually to identify changes. Segregate dules within the content workflow, implement and document compensating controls where segregation is not practical.	Workflow Segregation of Duties	MS-5.1 MS-5.2 MS-5.3 MS-6.1 MS-6.1	following areas at a minimum: I of security holden is and procedures • Content/Asset security and handling • Security holdent reporting and escalation • Disciplinary measures Establish a formal incident response plan that describes actions to be taken when a security incident is detected and reported identify the security incident response plan that describes actions to be taken when a security incident response plan that describes actions to be taken when a security incident response plan that describes actions to be taken when a security incident response team whow will be responsible for detecting analysing, and remediating security incident testes and the security incident response team 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 Document a workflow that includes the tracking of content at adultorization checkpoints throughout each process, include the following processes for both physical and digital content: • Delivery • Removal from the size • Destruction taentoly, implement, and assess the effectiveness of key contols to revervent, detect, and correct risks related to the content workflow Segregate duise within the content workflow, and implement and document compensating controls where segregation is not practical	between 2015 and 2013. 2015 MPAA added this control set. 2015 MPAA added this control set. The control requirements behind the control set did not change between 2015 and 2013. The control requirements behind the control set did not change between 2015 and 2013.
Business Continuity & Disaster Recovery Change Control & Configuration Management Workflow	MS-5.1 MS-5.2 MS-5.3 MS-6.0 MS-6.1 MS-6.0 MS-6.1 MS-8.0 MS-8.0 MS-8.1 MS-9.0	taken when a security incident is detected and reported. distrihly the security incident reported area who will be responsible for detecting, analysing, and remediating security incidents. Establish a security incident reporting process for individuals to report detected incidents to be security incident response team. Communicate incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client asset), and conduct a post-mortem meeting with management and client. Establish a formal plan that describes actions to be taken to ensure business continuity. Lientify the business continuity incident: Establish policies and procedures to ensure new data, applications, network, and systems components have been pre-approved by business leadership. Document workflows tracting content and authorization checkpoints. * Browgent * Browgent (sectify/teum) * Browgent * Browgent Lientify the business of both physical and digital content: * Deliver, (nectify/teum) * Browgent Lientify the section of the process, and review the workflow when there are changes to the process, and review the workflow process at least annually to identify changes. Segregate dules within the content workflow. Implement and document compensating controls where segregation is not practical. Perform background screening dhecks on all company personel and thing party works.	Workflow	M5.5.1 M5.5.2 M5.5.3 M5.6.0 M5.6.1 M5.6.1	following areas at a minimum:	between 2015 and 2013. 2015 MPAA added this control set. The control requirements behind the control set did not change between 2015 and 2013. The control requirements behind the control set did not change between 2015 and 2013. The control requirements behind the control set did not change between 2015 and 2013.
Business Continuity & Disaster Recovery Change Control & Configuration Management Workflow Segregation of Duties	MS-5.1 MS-5.2 MS-5.3 MS-6.0 MS-6.1 MS-6.0 MS-8.1 MS-8.1	taken when a security incident is detected and reported. identify the security incident reportes area who will be responsible for detecting, analysing, and remediating security incidents. Establish a security incident reporting process for individuals to report detected incidents to be security incident response team. Communicate incidents promptly to clients whose content may have been isaked, stolen or otherwise compromised (e.g., missing Client stols), and conduct a post-mortem meeting with management and client. Security and conduct a post-mortem meeting with management and client. Security and promptly taken who will be responsible for detecting, analysing and remediating controlinuly incidents. Establish policies, and procedures to ensure new data, applications, include the following processes for both physical and digital content: = believe (necelly return) = lowers: = Movement = Movement = Movement = Movement = Storage Update the workflow when there are changes to the process, and review the workflow process at least annually to identify changes. Segregate duise within the content workflow. Implement and document compensating controls where segregation is not practical. Perform background screening checks on all company personnel and	Workflow Segregation of Duties	MS-5.1 MS-5.2 MS-5.3 MS-6.1 MS-6.1	following areas at a minimum:	between 2015 and 2013. 2015 MPAA added this control set. 2015 MPAA added this control set. 2015 MPAA added this control set. The control requirements behind the control set did not change between 2015 and 2013. The control requirements behind the control set did not change between 2015 and 2013.
Business Continuity & Disaster Recovery Change Control & Configuration Management: Workflow Segregation of Duties Background Checks	MS-5.1 MS-5.2 MS-5.3 MS-6.0 MS-6.1 MS-6.0 MS-6.1 MS-8.0 MS-8.0 MS-8.1 MS-9.0	taken when a security incident is detected and reported. identify the security incident reportes area who will be responsible for detecting, analysing, and remediating security incidents. Establish a security incident reporting process for individuals to report detected incidents to the security incident response team. Communicate incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client sets), and conduct a poximoritem meeting with management and client. Establish a stormatic a poximoritem meeting with management and client. Establish policies, and procedures to ensure new data, applications, relations, communicating and remediated score that, applications, tendering, analysing and remediated score that, applications, include the following processes for both physical and digital content: • Bolewey (necles)/return) • Bogest • Boroage • Benovol(destruction • Storage • Removol(destruction • Storage • Removol(destruction • Regine all company personnel and regine all company personnel to a storage storage storage storage storage storage • Regine all company personnel to the process, and review the workflow upone there are changes to the process, and review the workflow process at least annually to identify changes. • Regine all company personnel and regine all company personnel and regine all company personnel and thind party worken.	Workflow Segregation of Duties Background Checks	M5.5.1 M5.5.2 M5.5.3 M5.6.0 M5.6.1 M5.6.1	following areas at a minimum: I of security pidders and procedures • Content/Asset security and handling • Sontent/Asset security and handling • Societarity incident response plan that describes actions to be taken when a security incident response plan that describes actions to be taken when a security incident response plan that describes actions to be taken when a security incident response plan that describes actions to be taken when a security incident response plan that describes actions to be taken when a security incident response plan that describes actions to be taken when a security incident response taken the security incident sequence taken whose content may have been leaked, stolen or otherwise compromised (e.g., missing client asset), and conduct a post-mortem meeting with management and client Document a workflow that includes the tracking of content and withorization checkpoints throughout each process, include the following processes for both physical and digital content: • Belivery • Bigest • Movement • Storage • Return to originator • Returd to origin	between 2015 and 2013. 2015 MPAA added this control set. 2015 MPAA added this control set. 2015 MPAA added this control set. The control requirements behind the control set did not change between 2015 and 2013. The control requirements behind the control set did not change between 2015 and 2013.
Business Continuity & Disaster Recovery Change Control & Configuration Management Workflow Segregation of Duties	MS-5.1 MS-5.2 MS-5.3 MS-6.0 MS-6.1 MS-6.0 MS-6.1 MS-8.0 MS-8.0 MS-8.1 MS-9.0	taken when a security incident is detected and reported. Gently the security incident reporte area who will be responsible for detecting, analysing, and remediating security incidents. Establish a security incident reporting process for individuals to report detected incidents to be security incident response team. Communicate incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client asset), and conduct a post-morter meeting with management and client. Establish a formatic a post-morter meeting with management and client. Establish is done and mendeliating controlluly incidents. Individe the biolowing and mendeliating controlluly incidents. Individe the following processes for both physical and digital content: • Bocument volt60ms tracking content and authorization checkpoints. Individe the following processes for both physical and digital content: • Bocument Volt60ms tracking content and authorization checkpoints. Bocument Volt60ms tracking content and authorization checkpoints. Bocument Volt60ms tracking content and authorization checkpoints. Bocument Volt60ms tracking content and authorization checkpoints. Saroage B temoval/destruction Update the workflow when there are changes to the process, and review the workflow process at least annually to identify changes. Sagregate dates within the content workflow, Implement and document compensating contools where segregation is not practical. Perform background screening decks on al company personnel and hird party workers. Require all company personnel to sign a confidentially agreement (e.g., non-disclosure) upon hire and annually thereafter, that includes requirements for handling and protecting content.	Workflow Segregation of Duties	M5.5.1 M5.5.2 M5.5.3 M5.6.0 M5.6.1 M5.6.1	following areas at a minimum: I of security pidders and procedures • Content/Asset security and handling • Security nicident response plan that describes actions to be taken when a security incident response plan that describes actions to be taken when a security incident response plan that describes actions to be taken when a security incident response plan that describes actions to be taken when a security incident response plan that describes actions to be taken when a security incident response plan that describes actions to be taken when a security incident response team who will be response blo detecting, analysing, and remdating security incident takets, and the security incident response team Communicate incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client aset), and conduct a post-morter meeting with management and client Discument a workflow that includes the tracking of content and authorization indeparts throughout act, process, include the following processes for both physical and digital content: • Delivery • Destruction 1 destruction 1 destruction 1 destruction Segregate duries within the content workflow Segregate duries within the content workflow Segregate duries within the content workflow, and implement and document compensating controls where segregation is not practical document compensating controls where segregation is not practical 4 document compensating controls where segregation is not practical and third party workers. Segregate duries within the content workflow, and implement and document compensating controls where segregation is not practical document compensating controls where segregation is not practical and third party workers.	between 2015 and 2013. 2015 MPAA added this control set. 2015 MPAA added this control set. 2015 MPAA added this control set. The control requirements behind the control set did not change between 2015 and 2013. The control requirements behind the control set did not change between 2015 and 2013. The control requirements behind the control set did not change between 2015 and 2013.
Business Continuity & Disaster Recovery Change Control & Configuration Management: Workflow Segregation of Duties Background Checks	MS-5.1 MS-5.2 MS-6.0 MS-6.1 MS-7.0 MS-8.0 MS-8.1 MS-9.0 MS-10.0 MS-11.0	taken when a security incident is detected and reported. Weintly the security incident reported area who will be responsible for detecting, analysing, and remediating security incidents. Establish a security incident reporting process for individuals to report detected incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client sates), and conduct a post-mortem meeting with management and client. Establish a formal plan that describes actions to be taken to ensure business continuity. Establish policies and procedures to ensure me with a, policiations, network, and systems content and authorization checkpoints. Nousement = slowage groups and remediating content and authorization checkpoints. network, and systems components have been pre-approved by business leadership. Document: = slowage = networkflow when there are changes to the process, and review the workflow process to host physical and digital content: = slowage = networkflow usen there are changes to the process, and review the workflow usen there are changes to the process, and review the workflow usen there are changes to the process, and review the workflow usen there are changes to the process, and review the workflow usen there are changes to the process, and review the workflow usen the content workflow. Implement and document compensating controls where segregation is not practical. Perform background screening thecks on all company personnel and thing party workers. Require all company personnel to sign a confidentiality agreement (e.g., Require all company personnel to sign a confidentiality agreement (e.g., nordisclower) public herad annually to identify changes.	Workflow Segregation of Duties Background Checks	MS-5.1 MS-5.2 MS-5.3 MS-6.0 MS	following areas at a minimum: I of security holders and procedures • Content/Asset security and handling • Security holder reporting and escalation • Disciplinary measures Establish a formal incident response plan that describes actions to be titlen when a security incident is detected and reported identify the security incident response plan that describes actions to be titlen when a security incident response plan that describes actions to be titlen when a security incident response plan that describes actions to be titlen when a security incident response team who will be responsible for detecting analysing, and remediating security incidents teated incidents to the security incident response team Communicate incidents prompting to clinicity of the security incident a workflow that includes the tracking of content and actent Document a workflow that includes the tracking of content and authorization checkpoints throughout each process; include the following processes for both physical and digital content: • Delivery • Ingest • Movement • Storage • Reguite authorization correct risks related to the content workflow the security indicent response the feactiveness of key controls to prevent, detect, and correct risks related to the content workflow segregate dues within the cortent workflow, and implement and document compensating contools where segregation is not practical Perform background screening mecks on all company personnel and thing any workers. Require all company personnel and thing party workers to sign a confidentiality agreent (e.g., modificiality party personnel and annually three after, that includes requirements for handing and protecting requires all company personnel and thing party workers to sign a confidentiality agreent (e.g., modificiality and protecting requires all company personnel and thing party workers to sign a confidentiality agreent (e.g., modificiality agreent (e.g., modificiality agreent (e.g., modificiality agreent (e.g., modificiality agr	between 2015 and 2013. 2015 MPAA added this control set. 2015 MPAA added this control set. 2015 MPAA added this control set. The control requirements behind the control set did not change between 2015 and 2013. The control requirements behind the control set did not change between 2015 and 2013.

The table below was created by AWS to highlight the delta between the MPAA best practices published in 2013 and the MPAA best practices published in 2013 and the MPAA best practices published in 2015. For any new control added to the 2015 MPAA best practices, see any rows highlighted in "green." For any control set which had a slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "green." For any control set which had a slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "blue." For any control set which had slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "blue." For any control set which has removed from the 2015 MPAA best practices, the controls were fulfighted in "green."

	MP/	AA Best Practices 2015		MP/	AA Best Practices 2013	AWS comments on the differences between 2015 and 2013 version
Security Topic	No. MS-12.1	Best Practice Require all third party workers to return all content and client	Security Topic	No. MS.S-10.0	Best Practice Communicate to clients the use of third-party storage providers for	and annual evaluation was removed.
		information in their possession upon termination of their contract.			physical assets	
	MS-12.2 MS-12.3	Include security requirements in third party contracts. Implement a process to reclaim content when terminating relationships.		MS-10.1 MS.S-10.1	Include security requirements in third party contracts Require international (to/from U.S.) transportation companies to be	
	11.5 12.5	implement a process to reclaim content when terminating relationships.		WIJ.J 10.1	"Customs-Trade Partnership Against Terrorism" (CTPAT) certified	
	MS-12.4	Require third party workers to be bonded and insured where appropriate (e.g., courier service).		MS-10.2	Implement a process to reclaim assets and remind third party workers of confidentiality agreements and contractual security requirements when	
					terminating relationships	
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.S-10.2	Re-assess transportation and packaging vendors annually and when the vendor changes its location and/or provides additional services	
	MS-12.6	Notify clients if subcontractors are used to handle content or work is		MS-10.3	Require third party workers to be bonded and insured where	
		offloaded to another company.		MS.S-10.3	appropriate (e.g., courier service) Review access to third-party content delivery systems and websites	
				MS-10.4	annually Restrict third party access to content/production areas unless required	
				MS.S-10.4	for their job function Incorporate security due diligence activities (e.g., security assessment,	
					self-assessment questionnaire) as part of a selection and hiring process for third party workers who handle sensitive content	
				MS-10.5	Require third party companies to notify clients if they are on-boarding	
	PS-1.0	Secure all entry/exit points of the facility at all times, including loading		PS-1.0	additional third party companies to handle content Lock all entry/exit points at all times if the facility does not have a	The MPAA 2015 has removed the requirements which specify the needs
	PS-1.1	dock doors and windows. Control access to areas where content is handled by segregating the		PS.S-1.0	segregated access-controlled area beyond reception Post security guards at all non-emergency entry/exit points	of a security guard, including the security patrols and investigation of incidents discovered by a security guard.
		content area from other facility areas (e.g., administrative offices, waiting rooms, loading docks, courier pickup and drop-off areas,			,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
	PS-1.2	replication and mastering). Control access where there are collocated businesses in a facility, which		PS-1.1	Control access to areas where content is handled by segregating the	
	1.5 1.2	includes but is not limited to the following: • Segregating work areas			content area from other facility areas (e.g., administrative offices)	
		Implementing access-controlled entrances and exits that can be				
Entry/Exit Points		segmented per business unit • Logging and monitoring of all entrances and exits within facility	Entry/Exit Points			
		 All tenants within the facility must be reported to client prior to engagement 				
				PS.S-1.1	Lock and install alarms on all loading dock doors, and monitor loading	
				PS.S-1.2	dock doors while in use Segregate the truck driver's entrance to prevent truck drivers from	
				PS.S-1.3	entering other areas of the facility Implement a daily security patrol process with a randomized schedule	
				PS.S-1.4	and document the patrol results in a log Document, investigate, and resolve all incidents detected during security	
	PS-2.0	Maintain a detailed visitors' log and include the following:		PS-2.0	guard shifts Maintain a detailed visitors' log which includes the following:	The control requirements behind the control set did not change
		Name Company			Name Company	between 2015 and 2013.
		Time in/time out Person/people visited			Time in/time out Person/people visited	
Visitor Entry/Exit		Signature of visitor Badge number assigned			Signature of visitor Badge number assigned	
Visitor Entry/Exit	PS-2.1	Assign an identification badge or sticker which must be visible at all	Visitor Entry/Exit	PS-2.1	Assign an identification badge or sticker, which must be visible at all	
	PS-2.2	times, to each visitor and collect badges upon exit. Do not provide visitors with key card access to content/production		PS-2.2	times, to each visitor and collect badges upon exit Do not provide visitors with electronic access to content/production	
	PS-2.3	areas. Require visitors to be escorted by authorized employees while on-site,		PS-2.3	areas Require visitors to be escorted by authorized employees while on-site,	
	PS-3.0	or in content/production areas. Provide company personnel and long-term third party workers (e.g.,		PS-3.0	or in content/production areas at a minimum Provide company personnel and long-term third party workers (e.g.,	The control requirements behind the control set did not change
Identification	1.5 5.0	janitorial) with a photo identification badge that is required to be visible at all times	Identification	15 5.0	janitorial) with photo identification that is validated and required to be visible at all times	between 2015 and 2013.
	PS-4.0	Implement perimeter security controls that address risks that the facility may be exposed to as identified by the organization's risk assessment.		PS-4.0	Implement perimeter security controls that address risks that the facility may be exposed to as identified by the organization's risk assessment	2015 MPAA has slight change in the perimeter security requirements, instead of having security guard stationed at the entrance/exits - the
	PS-4.1	Place security guards at perimeter entrances and non-emergency		PS.S-4.0	Install additional perimeter safeguards (e.g., fences, vehicle barricades)	standard is asking for a process w/randomized schedules.
Perimeter Security		entry/exit points.	Perimeter Security		to decrease the risk of unauthorized access onto the premises	
	PS-4.2	Implement a daily security patrol process with a randomized schedule and document the patrol results in a log.		PS.S-4.1	Lock perimeter gates at all times and dedicate an on-site employee to handle remote unlocking capabilities	
	PS-4.3	Lock perimeter gates at all times.		PS.S-4.2	Station a security guard at perimeter entrances and implement a process (e.g., electronic gate arm, parking permits) to allow vehicles into the	
	PS-5.0	Install a centralized, audible alarm system that covers all entry/exit		PS-5.0	facility campus Install a centralized, audible alarm system that covers all entry/exit	2015 MPAA has added the addition of fire safety measures in the event
		points (including emergency exits), windows, loading docks, fire escapes, and restricted areas (e.g., vault, server/machine room, etc.).			points (including emergency exits), loading docks, fire escapes, and restricted areas (e.g., vault, server/machine room)	of a power outage. Additionally, the alarms should be tested quarterly vs. semi-annually.
	PS-5.1	Install and effectively position motion detectors in restricted areas (e.g.,		PS-5.1	Configure alarms to provide escalation notifications directly to the	
		vault, server/machine room) and configure them to alert the appropriate security and other personnel (e.g. project managers, producer, head of			personnel in charge of security and/or be monitored by a central security group or third party	
		editorial, incident response team, etc.).			, 8,	
	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		PS-5.2	Assign unique arm and disarm codes to each person that requires access to the alarm system and restrict access to all other personnel	
		than a pre-determined period of time (e.g., 60 seconds).				
Alarms	PS-5.3	Configure alarms to provide escalation notifications directly to the personnel in charge of security and other personnel (e.g., project	Alarms	PS-5.3	Review the list of users who can arm and disarm alarm systems annually	
		managers, producer, head of editorial, incident response team, etc.).				
	PS-5.4	Assign unique arm and disarm codes to each person that requires access to the alarm system and restrict access to all other personnel.		PS-5.4	Test the alarm system every 6 months	
	PS-5.5	Review the list of users who can arm and disarm alarm systems		PS-5.5	Install and effectively position motion detectors in restricted areas (e.g.,	
		quarterly, or upon change of personnel.			vault, server/machine room) and configure them to alert the appropriate security personnel and/or third-party	
	PS-5.6	Test the alarm system quarterly.		PS-5.6	Install door prop alarms for content/production areas to notify when sensitive entry/exit points are open for longer than a pre-determined	
	PS-5.7	Implement fire safety measures so that in the event of a power outage,			period of time (e.g., 60 seconds)	
		fire doors fail open, and all others fail shut to prevent unauthorized access.				
	PS-6.0	Document and implement a process to manage facility access and keep records of any changes to access rights.		PS-6.0	Document and implement a process to manage facility access and keep records of any changes to access rights	2015 MPAA removed the requirement to review restricted access on a monthly basis.
	PS-6.1	Restrict access to production systems to authorized personnel only.		PS.S-6.0	Review access to restricted areas (e.g., vault, safe) on a monthly basis	
		contraction of the second s			and when the roles or employment status of any company personnel and/or third party workers change	
Authorization	PS-6.2	Review access to restricted areas (e.g., vault, server/machine room) guarterly and when the roles or employment status of company	Authorization	PS-6.1	Restrict access to production systems to authorized personnel only	
		personnel and/or third party workers are changed.		PS-6.2	Review access to restricted areas (e.g., vault, server/machine room)	
					quarterly and when the roles or employment status of company personnel and/or third party workers are changed	
	PS-7.0	Implement electronic access throughout the facility to cover all entry/exit points and all areas where content is stored, transmitted, or		PS-7.0	personnel and/or third party workers are changed Implement electronic access throughout the facility to cover all entry/exit points and all areas where content is stored, transmitted, or	2015 MPAA removed the requirement to implement separate rooms for replication and for mastering.
	PS-7.1	processed.		PS.S-7.0	processed	representation of mastering.
		Restrict electronic access system administration to appropriate personnel.			Establish separate rooms for replication and for mastering	
	PS-7.2	Store card stock and electronic access devices (e.g., keycards, key fobs) in a locked cabinet and ensure electronic access devices remain disabled		PS-7.1	Restrict electronic access system administration to appropriate personnel	
Electronic Access Control		prior to being assigned to personnel. Store unassigned electronic access devices (e.g., keycards, key fobs) in a locked cabinet and ensure these	Electronic Access			
		remain disabled prior to being assigned to personnel.				
	PS-7.3	Disable lost electronic access devices (e.g., keycards, key fobs) in the system before issuing a new electronic access device.			Store blank card stock in a locked cabinet and ensure keycards remain disabled prior to being assigned to personnel	

The table block was created by AVGS to highlight the defaultation of the AP practices published in 2013 and the MPAA best practices published in 2015. • For any new control added to the 2015 MPAA best practices, see any rows highlighted in "green." • For any control set which had a slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "green." • For any control set which had a slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "green." • For any control set which had a slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "blue." • For any control set which had for the 2014 MPAA best practices, see controls were highlighted in "green."

Formulas Texts		AA Best Practices 2015	for which and a	MP.	AA Best Practices 2013	AWS comments on the differences between 2015 and 2013 version
Security Topic	No. PS-7.4	Best Practice Issue third party access electronic access devices with a set expiration	Security Topic	No. PS-7.3	Best Practice Disable lost keycards in the system before issuing a new keycard	
		date (e.g. 90 days) based on an approved timeframe.		PS-7.4	Issue third party access cards with a set expiration date (e.g. 90 days)	
	PS-8.0	Limit the distribution of master keys and / or keys to restricted areas to authorized personnel only (e.g., owner, facilities management).		PS-8.0	based on an approved timeframe Limit the distribution of master keys to authorized personnel only (e.g., owner, facilities management)	2015 MPAA added additional controls on retrieving keys from terminated/third party employees. Additionally, the process of implementing electronic access controls and rekeying the entire facility
	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.		PS-8.1	Implement a check-in/check-out process to track and monitor the distribution of master keys	when a master key is lost.
Maria	PS-8.2	distribution of master keys and / or keys to restricted areas. Use keys that can only be copied by a specific locksmith for exterior entr//exit points.	Keys	PS-8.2	distribution of master keys 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	кеуз	PS-8.3	Inventory master keys and keys to restricted areas, including facility	
	PS-8.4	entry/exit points, quarterly. Obtain all keys from terminated employees/third-parties or those who			entry/exit points, quarterly	
	PS-8.5	no longer need the access. Implement electronic access control or rekey entire facility when master or sub-master keys are lost or missing.				
	PS-9.0	Install a CCTV system that records all facility entry/exit points and restricted areas (e.g. server/machine room, etc.).		PS-9.0	Install a CCTV system that records all facility entry/exit points and restricted areas	The control requirements behind the control set did not change between 2015 and 2013.
	PS-9.1	Review camera positioning and recordings to ensure adequate coverage, function, image quality, lighting conditions and frame rate of		PS.S-9.0	Review camera positioning, image quality, frame rate and retention daily	
	PS-9.2	surveillance footage at least daily. Restrict physical and logical access to the CCTV console and to CCTV		PS-9.1	Review camera positioning, image quality, lighting conditions, frame	
		equipment (e.g., DVRs) to personnel responsible for administering/monitoring the system.			rate, and adequate retention of surveillance footage at least weekly	
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	Cameras	PS.S-9.1	Designate an employee or group of employees to monitor surveillance footage during operating hours and immediately investigate detected	
		least 90 days, or the maximum time allowed by law, in a secure location.			security incidents	
	PS-9.4	Designate an employee or group of employees to monitor surveillance footage during operating hours and immediately investigate detected		PS-9.2	Restrict physical and logical access to the CCTV console and to CCTV equipment (e.g., DVRs) to personnel responsible for	
		security incidents.		PS-9.3	administering/monitoring the system Ensure that camera footage includes an accurate date and time-stamp	
	PS-10.0	Log and review electronic access to restricted areas for suspicious		PS-10.0	Log and review electronic access to restricted areas for suspicious	2015 MPAA removed the control regarding the retention of CCTV
	PS-10.1	events, at least weekly. Log and review electronic access, at least daily, for the following areas:		PS.S-10.0	events Perform a weekly review of electronic access logs for the following	surveillance footage.
		Masters/stampers vault Pre-mastering			areas, if applicable: • Masters/stampers vault	
		Server/machine room Scrap room			Pre-mastering Server/machine room	
Logging and Monitoring		High-security cages	Logging and Monitoring		Scrap room High-security cages	
	PS-10.2	Investigate suspicious electronic access activities that are detected.		PS-10.1	Investigate suspicious electronic access activities that are detected	
	PS-10.3	Maintain an ongoing log of all confirmed electronic access incidents and		PS-10.2	Maintain an ongoing log of all confirmed electronic access incidents and	
		include documentation of any follow-up activities that were taken.		PS-10.3	include documentation of any follow-up activities that were taken Retain CCTV surveillance footage and electronic access logs for at least	
				PS-10.3	90 days, or the maximum time allowed by law, in a secure location	
	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		PS-11.0	Inform company personnel and third party workers upon hire that bags and packages are subject to random searches and include a provision	The control requirements behind the control set did not change between 2015 and 2013.
	PS-11.1	content. Implement an exit search process that is applicable to all facility		PS.S-11.0	addressing searches in the facility policies Implement an exit search process that is applicable to all facility	between 2013 and 2013.
		Personnel and visitors, including: Removal of all outer coats, hats, and belts for inspection			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			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			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 			 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)	Searches	PS.S-11.1	Prohibit personnel from entering/exiting the facility with digital recording devices (e.g., USB thumb drives, digital cameras, cell phones)	
June 10.3		and include the search of these devices as part of the exit search procedure.	Junca		and include the search of these devices as part of the exit search procedure	
	PS-11.3	Enforce the use of transparent plastic bags and food containers for any food brought into production areas.			Enforce the use of transparent plastic bags and food containers for any food brought into production areas	
	PS-11.4	Implement a dress code policy that prohibits the use of oversized clothing (e.g., baggy pants, oversized hooded sweatshirts).		PS.S-11.3	Implement a dress code policy that prohibits the use of oversized clothing (e.g., baggy pants, oversized hooded sweatshirts)	
	PS-11.5	Use numbered tamper-evident stickers/holograms to identify authorized		PS.S-11.4	Use numbered, tamper-evident stickers/holograms to identify	
	PS-11.6 PS-11.7	devices that can be taken in and out of the facility. Implement a process to test the exit search procedure. Perform a random vehicle search process when exiting the facility		PS.S-11.5 PS.S-11.6	authorized devices that can be taken in and out of the facility Implement a process to test the exit search procedure Perform a random vehicle search process when exiting the facility	
	PS-11.8	parking lot. Segregate replication lines that process highly sensitive content and		PS.S-11.0	parking lot Segregate replication lines that process highly sensitive content and	
	PS-11.9	perform searches upon exiting segregated areas. Implement additional controls to monitor security guards activity.		PS.S-11.8	perform searches upon exiting segregated areas Implement additional controls to monitor security guard activity	
	PS-12.0	Implement a content asset management system to provide detailed		PS-12.0	Implement a content asset management system to provide detailed	2015 MPAA removed the requirement to use automated notification for
		tracking of physical assets (i.e., received from client created at the facility).			tracking of physical assets (i.e., client and newly created)	assets that have been out of the vault for extended periods of time. Additionally, added the requirement to Implement and review a daily
	PS-12.1	Barcode or assign unique tracking identifier(s) to client assets and created media (e.g., tapes, hard drives) upon receipt and store assets in		PS.S-12.0	Use automated notification for assets that have been out of the vault for extended periods of time	aging report to identify highly sensitive assets that are checked out from the vault and not checked back in.
	PS-12.2	the vault when not in use. Retain asset movement transaction logs for at least one year.		PS-12.1	- Barcode client assets and created media (e.g., tapes, hard drives) upon	
Inventory Tracking			Inventory Tracking		receipt and store assets in the vault when not in use	
,	PS-12.3	Review logs from content asset management system at least weekly and investigate anomalies.			Lock up and log assets that are delayed or returned if shipments could not be delivered on time	
	PS-12.4	Use studio film title aliases when applicable on physical assets and in asset tracking systems.		PS-12.2	Retain asset movement transaction logs for at least 90 days	
	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.		PS-12.3	Review logs from content asset management system and investigate anomalies	
	PS-12.6	Lock up and log assets that are delayed or returned if shipments could not be delivered on time.		PS-12.4	Use studio AKAs ("aliases") when applicable in asset tracking systems and on any physical assets	
	PS-13.0	Perform a quarterly inventory count of each client's asset(s), reconcile gainst asset management records, and immediately communicate		PS-13.0	Perform a quarterly inventory count of each client's pre-release project(s), reconcile against asset management records, and	2015 MPAA removed the requirement to perform a weekly inventory count of client's pre-release projects and the requirement to monitor
	PS-13.1	against asset management records, and immediately communicate variances to clients. Segregate duties between the vault staff and individuals who are		PS.S-13.0	project(s), reconcile against asset management records, and immediately communicate variances to clients Perform a weekly inventory count of each client's pre-release project(s),	film elements throughout the workflow process. Additionally, the
		responsible for performing inventory counts.			reconcile against asset management records, and immediately communicate variances to clients	the state of the s
Inventory Counts			Inventory Counts	PS-13.1	Segregate duties between the vault staff and individuals who are responsible for performing inventory counts	
				PS.S-13.1	Monitor film elements (e.g., negatives, unprocessed film) constantly throughout the workflow process	
				PS-13.2	Implement and review a daily aging report to identify highly sensitive assets that are checked out from the vault and not checked back in	
	PS-14.0	Tag (e.g., barcode, assign unique identifier) blank stock/raw stock per		PS-14.0	Tag (e.g., barcode, assign unique identifier) blank stock/raw stock per	The control requirements behind the control set did not change
Blank Media/ Raw Stock Tracking	PS-14.1	unit when received. Establish a process to track consumption of raw materials (e.g.,	Blank Media/ Raw Stock Tracking	PS.S-14.0	unit when received Establish a process to track consumption of raw materials (e.g.,	between 2015 and 2013.
	PS-14.2	polycarbonate) monthly. Store blank media/raw stock in a secured location.		PS-14.1	polycarbonate) monthly Store blank media/raw stock in a secured location	
	PS-15.0	Restrict access to finished client assets to personnel responsible for tracking and managing assets.		PS-15.0	Restrict access to finished client assets to personnel responsible for tracking and managing assets	2015 MPAA removes the requirement to use an access-controlled cage for the staging area and monitor the area with surveillance cameras
	PS-15.1	Store client assets in a restricted and secure area (e.g., vault, safe, or other secure storage location).		PS.S-15.0	Require two company personnel with separate access cards to unlock highly sensitive areas (e.g., safe, high-security cage) after-hours	
	PS-15.2	Require two company personnel with separate access cards to unlock		PS-15.1	Store client assets in a restricted and secure area (e.g., vault, safe)	
	DC 45 5	highly sensitive areas (e.g., safe, high-security cage) after-hours.				
Client Assets	PS-15.3	Use a locked fireproof safe to store undelivered packages that are kept at the facility overnight.	Client Assets	10.5-15.1	Use an access-controlled cage for the staging area and monitor the area with surveillance cameras	

The table below was created by AWS to highlight the delta between the MPAA best practices published in 2013 and the MPAA best practices published in 2013. For any new control addet to the 2015 MPAA best practices, see any rows highlighted in "green." • For any control set which had a slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "blue." • For any control set which had a slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "blue." • For any control set which had a slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "blue." • For any control set which has removed from the 2015 MPAA best practices, the controls were fundamentally unchanged.

	MP	AA Best Practices 2015		MP/	AA Best Practices 2013	AWS comments on the differences between 2015 and 2013 version
Security Topic	No. PS-15.4	Best Practice Implement a dedicated, secure area (e.g., security cage, secure room) for	Security Topic	No. PS.S-15.2	Best Practice Use a locked fireproof safe to store undelivered packages that are kept	
	P5-15.4	the storage of undelivered screeners that is locked, access-controlled,		P5.5-15.2	at the facility overnight	
		and monitored with surveillance cameras and/or security guards.				
				PS.S-15.3	Implement a dedicated, secure area (e.g., security cage, secure room) for	
					the storage of undelivered screeners that is locked, access-controlled, and monitored with surveillance cameras and/or security guards	
	PS-16.0	Require that rejected, damaged, and obsolete stock containing client		PS-16.0	Require that rejected, damaged, and obsolete stock are erased,	2015 MPAA does not specifically call out the requirements needed for
	-3-10.0	assets are erased, degaussed, shredded, or physically destroyed before		P3-10.0	degaussed, shredded, or physically destroyed before disposal (e.g., DVD	third parties. Nor the requirement to scratch discs before placing them
		disposal.			shredding, hard drive destruction) and update asset management records to reflect destruction	in the scrap bin.
	PS-16.1	Store elements targeted for recycling/destruction in a secure		PS.S-16.0	Implement a process that requires security personnel to monitor and	
		location/container to prevent the copying and reuse of assets prior to disposal.			record the scrapping process if scrap is destroyed	
	PS-16.2	Maintain a log of asset disposal for at least 12 months.		PS-16.1	Store elements targeted for recycling/destruction in a secure location/container to prevent the copying and reuse of assets prior to	
					disposal	
	PS-16.3	Destruction must be performed on site. On site destruction must be supervised and signed off by two company personnel. If a third party		PS.S-16.1	Conduct periodic security training for all company personnel and third party workers to educate on asset disposal and destruction processes	
Disposals		destruction company is engaged, destruction must be supervised and signed off by two company personnel and certificates of destruction	Disposals		(e.g., placing assets into designated containers)	
Dispositio		must be retained.	Dispositio			
	PS-16.4	Use automation to transfer rejected discs from replication machines directly into scrap bins (no machine operator handling).		PS-16.2	Maintain a log of asset disposal for at least 12 months	
				DS 5 16 7	Scratch discs before placing them into the scrap bin	
				PS-16.2 PS-16.3	Require third-party companies who handle destruction of content to	
					provide a certificate of destruction for each completed job	
				PS.S-16.3	Use automation to transfer rejected discs from replication machines	
					directly into scrap bins (no machine operator handling)	
				PS.S-16.4	Prohibit the use of third party companies for the destruction of DCDM drives or pre-released content	
	PS-17.0	Require the facility to generate a valid work/shipping order to authorize		PS-17.0	Require the facility to file a valid work/shipping order to authorize asset	2015 MPAA requires assets in transit are tracked and logged with
	PS-17.1	client asset shipments out of the facility. Track and log client asset shipping details; at a minimum, include the		PS.S-17.0	shipments out of the facility Document and retain a separate log for truck driver information	shipping details.
		following: • Time of shipment				
		 Sender name and signature 				
		Recipient name Address of destination				
		Tracking number from courier				
	PS-17.2	 Reference to the corresponding work order Secure client assets that are waiting to be picked up. 		PS-17.1	Track and log asset shipping details; at a minimum, include the	
					following: • Time of shipment	
					Sender name and signature	
					Recipient name Address of destination	
					 Tracking number from courier 	
Shipping			Shipping		Reference to the corresponding work order	
	PS-17.3	Validate client assets leaving the facility against a valid work/shipping		PS.S-17.1	Require personnel picking up package(s) to verify the count the	
		order.			shipping document and obtain a signature from the shipping point	
	PS-17.4	Prohibit couriers and delivery personnel from entering content/production areas of the facility.		PS-17.2	Validate assets leaving the facility against a valid work/shipping order	
	PS-17.5	Document and retain a separate log for truck driver information.		PS.S-17.2	Observe and monitor the packing and sealing of trailers when shipping	
	PS-17.6	Observe and monitor the on-site packing and sealing of trailers prior to		PS-17.3	occurs on-site Secure assets that are waiting to be picked up	
	PS-17.7	shipping. Record, monitor and review travel times, routes, and delivery times for		PS.S-17.3	Implement a formal process to record, monitor, and review travel times,	
	-3-17.7	shipments between facilities.		F3.3-17.3	routes, and delivery times for shipments between facilities	
	PS-17.8	Prohibit the transfer of film elements other than for client studio		PS-17.4	Prohibit couriers and delivery personnel from entering	
		approved purposes.			content/production areas of the facility	
	PS-17.9	Ship prints for pre-theatrical screenings in segments (e.g., odd versus even reels).			Do not allow film elements to leave the facility other than through shipping, except with a signed authorization pass	
				PS.S-17.5	Ship prints for pre-theatrical screenings in segments (e.g., odd versus even reels)	
	PS-18.0	Inspect delivered client assets upon receipt and compare to shipping documents (e.g., packing slip, manifest log).		PS-18.0	Inspect delivered content upon receipt and compare to shipping documents (e.g., packing slip, manifest log)	The control requirements behind the control set did not change between 2015 and 2013.
	PS-18.1	Maintain a receiving log to be filled out by designated personnel upon		PS-18.1	Maintain a receiving log to be filled out by designated personnel upon	between 2015 and 2013.
	PS-18.2	receipt of deliveries. Perform the following actions immediately:		PS-18.2	receipt of deliveries Perform the following actions immediately:	
Receiving		Tag (e.g., barcode, assign unique identifier) received assets	Receiving		 Tag (e.g., barcode, assign unique identifier) received assets, 	
		 Input the asset into the asset management system Move the asset to the restricted area (e.g., vault, safe) 			 Input the asset into the asset management system Move the asset to the restricted area (e.g., vault, safe) 	
	PS-18.3	Implement a secure method for receiving overnight deliveries.		PS-18.3	Implement a secure method (e.g., secure drop box) for receiving overnight deliveries	
	PS-19.0	Prohibit the use of title information, including AKAs ("aliases"), on the		PS-19.0	Prohibit the use of title information, including AKAs ("aliases"), on the	The control requirements behind the control set did not change
Labeling	1	outside of packages unless instructed otherwise by client.	Labeling		outside of packages	between 2015 and 2013.
	PS-20.0	Ship all client assets in closed/sealed containers, and use locked		PS-20.0	Ship all assets in closed/sealed containers, and use locked containers	The control requirements behind the control set did not change
1	1	containers depending on asset value, or if instructed by the client.			depending on asset value	between 2015 and 2013.
1	PS-20.1	Implement at least one of the following controls: • Tamper-evident tape		PS.S-20.0	Apply shrink wrapping to all shipments, and inspect packaging before final shipment to ensure that it is adequately wrapped	
	1	Tamper-evident packaging			mus supriment to ensure that it is adequately wrapped	
Packaging	1	 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.		PS-20.1	Implement at least one of the following controls:	
1	1	mai supment to ensure that it is adequately wrapped.			Tamper-evident tape Tamper-evident packaging	
1	1				 Tamper-evident seals in the form of holograms Secure containers (e.g., Pelican case with a combination lock) 	
	PS-21.0	Lock automobiles and trucks at all times, and do not place packages in		PS-21.0	Lock automobiles and trucks at all times, and do not place packages in	The control requirements behind the control set did not change
	PS-21.1	clear view. Include the following security features in transportation vehicles (e.g.,		PS.S-21.0	visible auto/truck areas Include the following security features in transportation vehicles (e.g.,	between 2015 and 2013.
	1	trailers): • Segregation from driver cabin			trailers): • Segregation from driver cabin	
Transport Vehicles	1	 Ability to lock and seal cargo area doors 	Transport Vehicles		 Ability to lock and seal cargo area doors 	
1	PS-21.2	 GPS for high-security shipments Apply numbered seals on cargo doors for shipments of highly sensitive 		PS.S-21.1	 GPS for high-security shipments Apply numbered seals on cargo doors for shipments of highly sensitive 	
1	PS-21.3	titles. Require security escorts to be used when delivering highly sensitive		PS.S-21.2	titles Require security escorts be used for delivery of highly sensitive content	
		content to high-risk areas.			in high-risk areas	
	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		DS-1.0	Segment WAN(s) by using stateful inspection firewalls with Access Control Lists that prevent unauthorized access to any internal network	2015 MPAA added the requirements to perform quarterly vuln scans of external IP ranges, secure any point to point connections by using
		unauthorized access to any internal network and with the ability to keep un with upload and download traffic				dedicated, private connections and by using encryption. Additionally the
						requirement to implement baseline security requirements for WAN network infrastructure devices and services.
	DS-1.1	Implement a process to review firewall Access Control Lists (ACLs) to confirm configuration settings are appropriate and required by the		DS-1.1	Develop a process to review firewall Access Control Lists (ACLs) to confirm configuration settings are appropriate and required by the	
		business every 6 months.			business every 6 months	
	DS-1.2	Deny all protocols by default and enable only specific permitted secure protocols to access the WAN and firewall.		DS-1.2	Deny all protocols by default and enable only specific permitted secure protocols on the WAN	
	DS-1.3	Place externally accessible servers (e.g., web servers) within the DMZ.		DS-1.3	Place externally accessible servers (e.g., secure FTP server, web servers)	
	DS-1.4	Implement a process to patch network infrastructure devices (e.g.,		DS-1.4	within the DMZ 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.			firewalls, routers, switches, etc.) regularly	
	DS-1.5	Harden network infrastructure devices, SAN/NAS, and servers based on		DS-1.5	Harden network infrastructure devices based on security configuration	
Firewall/WAN/		security configuration standards. Disable SNMP (Simple Network Management Protocol) if it is not in use or use only SNMPv3 or higher			standards	
Perimeter Security		and select SNMP community strings that are strong passwords.	WAN			
	DS-1.6	Do not allow remote management of the firewall from any external		DS-1.6	Do not allow remote access to WAN network infrastructure devices (e.g.,	
		interface(s).			firewall, router) that control access to content	

The table below was created by AWS to highlight the delta between the MPAA best practices published in 2013 and the MPAA best practices published in 2013 and the MPAA best practices published in 2015. For any new control added to the 2015 MPAA best practices, see any rows highlighted in "green." For any control set which had a slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "green." For any control set which had a slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "blue." For any control set which had slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "blue." For any control set which has removed from the 2015 MPAA best practices, the controls were fulfighted in "green."

Security Topic	MP	AA Best Practices 2015		MP.	AA Best Practices 2013	AWS comments on the differences between 2015 and 2013 version
	No. DS-1.7	Best Practice Secure backups of network infrastructure/SAN/NAS devices and servers	Security Topic	No. DS-1.7	Best Practice Secure backups of network infrastructure devices to a centrally secured	
	DS-1.7	Secure backups of network infrastructure/SAN/NAS devices and servers to a centrally secured server on the internal network.		JS-1.7	Secure backups of network infrastructure devices to a centrally secured server on the internal network	
	DS-1.8	Perform quarterly vulnerability scans of all external IP ranges and hosts		DS-1.8	Perform an annual vulnerability scan on hosts that are externally	
	DS-1.9	at least and remediate issues. Perform annual penetration testing of all external IP ranges and hosts at		DS-1.9	accessible and remediate issues Allow only authorized personnel to request the establishment of a	
		least and remediate issues.		03-1.9	connection with the telecom service provider	
	DS-1.10	Secure any point to point connections by using dedicated, private connections and by using encryption.				
	DS-1.11	Implement a synchronized time service protocol (e.g., Network Time Protocol) to ensure all systems have a common time reference.				
	DS-1.12	Establish, document and implement baseline security requirements for				
	05-1.12	WAN network infrastructure devices and services.				
	DS-2.0	Prohibit production network and all systems that process or store digital		DS-2.0	Prohibit Internet access on systems (desktops/ servers) that process or	The control requirements behind the control set did not change
		content from directly accessing the internet, including email. If a business case requires internet access from the production network or			store digital content	between 2015 and 2013.
		from systems that process or store digital content, only approved				
		methods are allowed via use of a remote hosted application / desktop session.				
	DS-2.1	Implement email filtering software or appliances that block the following from non-production networks:		DS-2.1	Implement e-mail filtering software or appliances that block the following from non-production networks:	
Internet		Potential phishing emails Prohibited file attachments (e.g., Visual Basic scripts, executables, etc.)	Internet		Potential phishing e-mails Prohibited file attachments (e.g., Visual Basic scripts, executables, etc.)	
		 File size restrictions limited to 10 MB 			Frontibilities the attachments (e.g., visual basic scripts, executables, etc.) File size restrictions limited to 10 MB	
		Known domains that are sources of malware or viruses				
	DS-2.2	Implement web filtering software or appliances that restrict access to		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			websites known for peer-to-peer file trading, viruses, hacking or other malicious sites	
	DS-3.0	Isolate the content/production network from non-production networks		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.			(e.g., office network, DMZ, etc.) by means of physical or logical network segmentation	Network: • Use switches/layer 3 devices to manage the network traffic, and
						disable all unused switch ports • Restrict the use of non-switched devices on the content/production
	DS-3.1	Restrict access to the content/production systems to authorized		DS-3.1	Restrict access to the content/production systems to authorized	network.
	DS-3.2	personnel. Restrict remote access to the content/production network to only		DS-3.2	personnel Restrict remote access to the content/production network to only	Disable SNMP if it is not in use Harden systems
		approved personnel who require access to perform their job responsibilities.			approved personnel who require access to perform their job responsibilities	Conduct internal network vulnerability scans Secure backups of local area network SAN/NAS, devices, servers and
	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		DS-3.3	Disable all unused switch ports on the content/production network to prevent packet sniffing by unauthorized devices	workstations to a centrally secured server on the internal network.
		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	DS-3.4	Restrict the use of non-switched devices such as hubs and repeaters on the content/production network	
	DS-3.5	Prohibit dual-homed networking (physical networked bridging) on computer systems within the content/production network.		DS-3.5	Prohibit dual-homed networking (network bridging) on computer systems within the content/production network	
	DS-3.6	Implement a network-based intrusion detection /prevention system		DS-3.6	Implement a network-based intrusion detection or prevention system	
	DS-3.7	(IDS/IPS) on the content/production network. Disable SNMP (Simple Network Management Protocol) if it is not in use			on the content/production network	
		or uses only SNMPv3 or higher and select SNMP community strings that are strong passwords.				
	DS-3.8	Harden systems prior to placing them in the LAN / Internal Network.				
	DS-3.9	Conduct internal network vulnerability scans and remediate any issues,				
	DS-3.10	at least annually. Secure backups of local area network SAN/NAS, devices, servers and				
		workstations to a centrally secured server on the internal network.				
	DS-4.0	Prohibit wireless networking and the use of wireless devices on the		DS-4.0	Prohibit wireless networking and the use of wireless devices on the	The control requirements behind the control set did not change
	DS-4.1	content/production network. Configure non-production wireless networks (e.g., administrative and		DS-4.1	production/content network Configure non-production wireless networks (e.g., administrative and	between 2015 and 2013.
		guest) with the following security controls: • Disable WEP / WPA			guest) with the following security controls: • Disable WEP	
Wireless/WLAN		Only Enable AES128 encryption (WPA2), or higher	Wireless		Enable AES encryption	
		Segregate "guest" networks from the company's other networks Change default administrator logon credentials			Segregate "guest" networks from the company's other networks	
		Change default network name (SSID)				
	DS-4.2	Implement a process to scan for rogue wireless access points and remediate any validated issues.		DS-4.2	Implement a process to scan for rogue wireless access points annually	
	DS-5.0	Designate specific systems to be used for content input/output (I/O).		DS-5.0	Designate specific systems to be used for content input/output (I/O)	2015 MPAA removed the requirement to restrict the installation and or/use of media burners.
	DS-5.1	Block input/output (I/O), mass storage, external storage, and mobile		DS-5.1	Block input/output (I/O) devices (e.g., USB, FireWire, e-SATA, SCSI, etc.)	oryase of mean particis.
		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			on all systems that handle or store content, with the exception of systems used for content I/O	
I/O Device Security		handle or store content, with the exception of systems used for content I/O.	I/O Device Security			
					Restrict the installation and/or use of media burners (e.g., DVD, Blu-ray,	
				DS-5.2		
	DS-6.0			DS-5.2	CD burners) and other devices with output capabilities to specific I/O systems used for outputting content to physical media	
		Install anti-virus and anti-malware software on all workstations, servers,		DS-5.2 DS-6.0		2015 MPAA requires a inventory of system components and a
		Install anti-virus and anti-malware software on all workstations, servers, and on any device that connects to SAN/NAS systems.			systems used for outputting content to physical media	2015 MPAA requires a inventory of system components and a documented network topology.
	DS-6.1	and on any device that connects to SAN/NAS systems. Update all anti-virus and anti-malware definitions daily, or more			systems used for outputting content to physical media	
	DS-6.1 DS-6.2	and on any device that connects to SAN/NAS systems. Update all anti-virus and anti-malware definitions daily, or more frequently. Scan all content for viruses and malware prior to ingest onto the		DS-6.0 DS-6.1	systems used for outputting content to physical media Install anti-virus software on all workstations and servers Update anti-virus definitions daily Scan file-based content for viruses prior to ingest onto the	
		and on any device that connects to SAN/NAS systems. Update all anti-virus and anti-malware definitions daily, or more frequently.		DS-6.0 DS-6.1 DS-6.2	systems used for outputting content to physical media Install anti-virus software on all workstations and servers Update anti-virus definitions daily	
	DS-6.2	and on any device that connects to SAV/NAS systems. Update all anti-virus and anti-malware definitions daily, or more frequently. Scan all content for viruses and malware prior to ingest onto the content/production network. Perform scans as follows: – Enable regular full system virus and malware scanning on all		DS-6.0 DS-6.1 DS-6.2	systems used for outputting content to physical media Install anti-virus software on all workstations and servers Update anti-virus definitions daily Scan file-based content, for viruses prior to ingest onto the content/production network Performing virus scans as follows: - Inable regular file system virus scanning on all workstations	
	DS-6.2	and on any device that connects to SAV/NAS systems. Update all anti-virus and anti-malware definitions daily, or more frequently. Scan all content for viruses and malware prior to ingest onto the content/production network. Perform scans as follows: E nable regular full system virus and malware scanning on all workstations = finable rigid system virus and malware scans for servers and for systems		DS-6.0 DS-6.1 DS-6.2	systems used for outputting content to physical media Install anti-virus software on all workstations and servers Update anti-virus definitions daily Scan file-based content for viruses prior to ingest onto the content/production network Performing virus can as follows:	
	DS-6.2	and on any device that connects to SAV/NAS systems. Update all anti-virus and anti-malware definitions daily, or more frequently. Scan all content for viruses and malware prior to ingest onto the content/production network. Perform scans as follows: Enable regular hill system virus and malware scanning on all workstations Enable frequip risystem virus and malware scans for servers and for systems connecting to a SAV/NAS Implement a process to regularly update systems (e.g., file transfer		DS-6.0 DS-6.1 DS-6.2	systems used for outputting content to physical media Install anti-virus software on all workstations and servers Update anti-virus definitions daily Scan file-based content for viruses prior to ingest onto the content/production network Performing virus cans as follows: • Enable regular full system virus scanning on all workstations	
	DS-6.2 DS-6.3	and on any device that connects to SAN/NAS systems. Update all anti-virus and anti-malware definitions daily, or more frequently. Scan all content for viruses and malware prior to ingest onto the content/production network. Perform scans as follow: • Enable regular full system virus and malware scanning on all workstations • Enable full system virus and malware scans for severes and for systems connecting to 35 M/NAS Implement a process to regularly update systems (eds., file transfer systems, operating systems, databases, applications, network devices)		DS-6.0 DS-6.1 DS-6.2 DS-6.3	systems used for outputting content to physical media Install anti-virus software on all workstations and servers Update anti-virus definitions daily Scan file-based content for viruses prior to ingest onto the content/production network Performing virus scans as follows: • Enable regular full system virus scanning on all workstations • Enable regular thil system virus scans for servers, where applicable (e.g., non- SAN systems) Implement a process to regularly update systems (e.g., file transfer	
	DS-6.2 DS-6.3 DS-6.4	and on any device that connects to SAV/NAS systems. Update all anti-virus and anti-malware definitions daily, or more frequently. Scan all content for viruses and malware prior to ingest onto the content/strondcome network. Perform scams as follows: = nable regular this system virus and malware scanning on all we smalle fully independent of the system virus and malware scanning on all we smalle fully system virus and malware scans for servers and for systems connecting to 3-SM/NAS. Implement a process to regularly update systems (e.g., file transfer systems, operating systems, distabases, applications, network device) with patches/updates that remediate security vulnerabilities.		DS-6.0 DS-6.1 DS-6.2 DS-6.3 DS-6.4	systems used for outputting content to physical media Install anti-virus software on all workstations and servers Update anti-virus definitions daily Scan file-based content for viruses prior to ingest onto the content/production network. Performing virus scans as follows: • Enable regular full system virus scanning on all workstations • Enable full system virus scans for servers, where applicable (e.g., non- SAN systems) Implement a process to regularly update systems (e.g., file transforms) storess, toperaling systems, database, application, tendows devices) with patches/updates that remediate security vulnerabilities	
	DS-6.2 DS-6.3 DS-6.4	and on any device that connects to SAV/NAS systems. Update all anti-virus and anti-malware definitions daily, or more frequently. Scan all content for viruses and malware prior to ingest onto the content/production network. Perform scans as follows: a Snable regular this system virus and malware scanning on all workstations and shall by system virus and malware scans for servers and for systems and shall by system virus and malware scans for servers and for systems and shall by system virus and malware scans for servers and for systems systems, operanding systems, database, spolications, enework derices] with parches/updates that remediate socurity vulnerabilities. Prohibit users from being administrators on their own workstations, miss required for software (e.g., Proofs). (Eighter an authoring		DS-6.0 DS-6.1 DS-6.2 DS-6.3	systems used for outputting content to physical media Install anti-virus software on all workstations and servers Update anti-virus definitions daily Scan file-based content for viruses prior to ingest onto the content/production network Performing virus scans as follows: • Enable regular full system virus scanning on all workstations • Enable regular thil system virus scans for servers, where applicable (e.g., non- SAN systems) Implement a process to regularly update systems (e.g., file transfer	
	DS-6.2 DS-6.3 DS-6.4	and on any device that connects to SAV/NAS systems. Update all anti-virus and anti-malware definitions daily, or more frequently. Scan all content for viruses and malware prior to ingest onto the content/production network. Perform scans as follows: Enable regular full system virus and malware scanning on all workstations Enable frequier full system virus and malware scans for servers and for systems connecting to a SAV/NAS Implement a process to regularly update systems (e.g., file transfer systems, operating systems, databases, applications, network devices) with patche/updates that remediate security vulnerabilities. Prohibit users from being Administrators on their own workstatons, unless required for software (e.g., ProTocis, Clipster and authoring software such as Bu-irvirus, Scansifa and Tochsha). Documentation from		DS-6.0 DS-6.1 DS-6.2 DS-6.3 DS-6.4	systems used for outputting content to physical media Install anti-virus software on all workstations and servers Update anti-virus definitions daily Scan file-based content for viruses prior to ingest onto the content/production network. Performing virus scans as follows: • Enable regular full system virus scanning on all workstations • Enable full system virus scans for servers, where applicable (e.g., non- SAN systems) Implement a process to regularly update systems (e.g., file transforms) storess, toperaling systems, database, application, tendows devices) with patches/updates that remediate security vulnerabilities	
System Security	DS-6.2 DS-6.3 DS-6.4 DS-6.5	and on any device that connects to SAV/NAS systems. Update all anti-virus and anti-malware definitions daily, or more frequently. Scan all content for viruses and malware prior to ingest onto the content/production network. Perform scans as follows: E-nable regular full system virus and malware scanning on all workstations E-nable full system virus and malware scans for servers and for systems connecting to 3 SAV/NAS 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. Prohibit users from being daministrations on their own workstations, unless required for software (e.g., ProTools, Clipster and authoring software such as Bur-firvi, Senavista and Toshiba). Documentation from the software provider must explicitly state that administrative rights are required.	System Security	DS-6.0 DS-6.1 DS-6.2 DS-6.3 DS-6.4 DS-6.5	systems used for outputting content to physical media Install anti-virus software on all workstations and servers Update anti-virus definitions daily Scan file-based content, for viruses prior to ingest onto the content/production network. Performing virus cars as follows: = nailee full system virus scanning on all workstations = naibe full system virus scann for exercis, where applicable (e.g., non- SAN system) Implement a process to regularly update systems (e.g., file transfer systems, operating systems, databases, applications, network devices) with patche/updates that remediate security vulnerabilities Prohibit users from being Administrators on their own workstations	
System Security	DS-6.2 DS-6.3 DS-6.4	and on any device that connects to SAV/NAS systems. Update all anti-virus and anti-malware definitions daily, or more frequently. Scan all content for viruses and malware prior to ingest onto the content/production network. Perform scans as follows: I challe regular this system virus and malware scanning on all workstations E challe help system virus and malware scans for servers and for systems connecting a social system virus and malware scans for servers and for systems connecting a social system virus and malware scans for servers and for systems connecting a social system virus and malware scans for servers and for systems connecting a social system virus and malware scans for servers and for systems connecting a social system virus and malware systems (device) systems, operaning systems, distabase, segulations, retwork devices with patches/updates that remediate security vulnerabilities. Prohbit users from being administrators on their own workstations, unless required for software (e.g., Proc). Clipster and automing software such as Bur-Frint. Scenarist and Toshiba). Documentation from	System Security	DS-6.0 DS-6.1 DS-6.2 DS-6.3 DS-6.4 DS-6.5	systems used for outputting content to physical media Install anti-virus software on all workstations and servers Update anti-virus definitions daily Scan file-based content for viruses prior to ingest onto the content/production network. Performing virus scans as follows: • Enable regular full system virus scanning on all workstations • Enable full system virus scans for servers, where applicable (e.g., non- SAN systems) Implement a process to regularly update systems (e.g., file transforms) storess, toperaling systems, database, application, tendows devices) with patches/updates that remediate security vulnerabilities	
System Security	DS-6.2 DS-6.3 DS-6.4 DS-6.5	and on any device that connects to SAV/NAS systems. Update all anti-virus and anti-malware definitions daily, or more frequently. Scan all content for viruses and malware prior to ingest onto the content/ground content on etwork. Perform scans as follows: Enable regular hill system virus and malware scanning on all workstations Enable fully englet the system scans for servers and for systems Connecting to a SAV/NAS implement a process to regularize scans for servers and for systems connecting to a SAV/NAS in the atthe system scans to regularize scans for servers and the patcher scanses to regularize scanse (e.g., life transfer invitems, operating system, classes, applications, network derices) with atthe scale scanse starter endeates security vulnerabilities. Prohibit users from being Administrators on their own workstations, unless required for Software (e.g., Proc)C, Clipster and authoring software such as Bur-Frint, Scensist and Toshiba). Documentation from is oftware for out must enplicitly state that administrative registrates.	System Security	DS-6.0 DS-6.1 DS-6.2 DS-6.3 DS-6.4 DS-6.5	systems used for outputting content to physical media Install anti-virus offware on all workstations and servers Update anti-virus definitions daily Scan file based content for viruses prior to ingest onto the content/production network Performing virus scans as follows: • Enable reguler flusystem virus scanning on all workstations • Enable full system virus scans for servers, where applicable (e.g., non- SAV systems) Implement a process to regularly update systems (e.g., file transfer systems, operating systems, databaset, applicables, network devices) Into active durates that drendate accurity vulnerballities Prohibit users from being Administrators on their own workstations Use cable locks on portable computing devices that handle content (e.g.,	
System Security	DS-6.2 DS-6.3 DS-6.4 DS-6.5 DS-6.6	and on any device that connects to SAV/NAS systems. Update all anti-virus and anti-malware definitions daily, or more frequently. Scan all content for viruses and malware prior to ingest onto the content/groduction network. Perform scans as follows: Enable regular hill system virus and malware scanning on all workstations Enable regular hill system virus and malware scanning on all workstations Enable regular biostem virus and malware scans for servers and for systems connecting to a SAV/NAS implement a process to regularly update systems (e.g., file transfer systems, operating systems, atabases, applications, network devices) with patchely/update shart remediate security wirershiftens. Prohibit usars from being Administrators on their own workstations, software such as Biu-Print, Scensist and Tachiba). Documentation from is onbuare provider must explicitly state that administrative rights are required. List cable locks on portable computing devices that handle content (e.g., laptas, tablets, towers) when they are left unattended. Implement additional security controls for laptops and portable computing storage devices that contaction center of sensity endormal	System Security	DS-6.0 DS-6.1 DS-6.2 DS-6.3 DS-6.4 DS-6.5 DS-6.6	systems used for outputting content to physical media Install anti-virus offware on all workstations and servers Update anti-virus definitions daily Scan life based content for viruses prior to ingest onto the content/production network Performing virus scans as follows: • nable regular hisystem virus scanning on all workstations • nable flui system virus scanns for servers, where applicable (e.g., non- SM systems) Insplement a process to regularly update systems (e.g., file transfer systems, operating systems, databases, applicables, network devices) Introplement process to regularly update systems (e.g., file transfer systems, operating systems, databases, applicables, network devices) Prohibit users from being Administrators on their own workstations Use cable locks on portable computing devices that handle content (e.g., laptops, tablets, towers) when they are left unattended	
System Security	DS-6.2 DS-6.3 DS-6.4 DS-6.5 DS-6.6	and on any device that connects to SAV/NAS systems. Update all anti-virus and anti-malware definitions daily, or more frequently. Scan all content for viruses and malware prior to ingest onto the content/production network. Perform scans as follows: Enable regular hill system virus and malware scanning on all workstations Enable regular hill system virus and malware scans for severs and for systems connecting to a SAV/NAS implement a process to regularly update systems (e.g., file transfer systems, operating systems, databases, applications, network devices) with patchely-updates that remediate accumy viruershilters. Prohibit usars from being Administrators on their own workstations, ensormed and the software (e.g., ProcOS. Clipskin we databases, and the software growider must explicitly state that administrative rights are required. Lipscable toks on portable computing devices that handle content (e.g., laptops, tablets, towers) when they are left unattended. Implement additional security controls for laptops and portable computing torage devices that contain calls and portable computing torage devices that contain client or sensitive registra relations.	System Security	DS-6.0 DS-6.1 DS-6.2 DS-6.3 DS-6.4 DS-6.5 DS-6.6	systems used for outputting content to physical media Install anti-virus offware on all workstations and servers Update anti-virus definitions daily Scan life baded content for viruses prior to ingest onto the content/production network Performing virus scans as follows: • Inable regular hisystem virus scanning on all workstations • Inable fill system virus scanns for servers, where applicable (e.g., non- SAV systems) Insplement a process to regularly update systems (e.g., file transfer systems, operating systems, databases, applicable (e.g., non- SAV systems) Insplement a process to regularly update systems (e.g., file transfer systems, operating systems, databases, applicables, network devices) Prohibit users from being Administrators on their own workstations Use cable locks on portable computing devices that handle content (e.g., laptops, tablets, towers) when they are left unattended Intall remote-kill software on all portable computing devices that stonge	
System Security	DS-6.2 DS-6.3 DS-6.4 DS-6.5 DS-6.6	and on any device that connects to SAV/NAS systems. Update all anti-virus and anti-malware definitions daily, or more frequently. Scan all content for viruses and malware prior to ingest onto the content/production network. Perform stams as follow: - Enable regular his system virus and malware scanning on all - Enable full system virus and malware scanning on all - Enable full system virus and malware scans for servers and for systems connecting to 35 MVMAS implement a process to regularly update systems (e.g., file transfer systems, operaning systems, databases, applications, retwork device) with patche/updates that remediate security vulnerabilities. Prohibit users from being Administrators on their own workstations, unless required for must equicity that that administrations coltware such as Bin-Print, Scenarist and Toshiba). Documentation from the cable locks on portable computing devices that handle content (e.g., luptosa), tablets, tomery when they are left unattended. Implement additional security controls for splops and portable computing conge devices that contain content or sensitive information required.	System Security	DS-6.0 DS-6.1 DS-6.2 DS-6.3 DS-6.4 DS-6.5 DS-6.6	systems used for outputting content to physical media Install anti-virus offware on all workstations and servers Update anti-virus definitions daily Scan life baded content for viruses prior to ingest onto the content/production network Performing virus scans as follows: • Inable regular hisystem virus scanning on all workstations • Inable fill system virus scanns for servers, where applicable (e.g., non- SAV systems) Insplement a process to regularly update systems (e.g., file transfer systems, operating systems, databases, applicable (e.g., non- SAV systems) Insplement a process to regularly update systems (e.g., file transfer systems, operating systems, databases, applicables, network devices) Prohibit users from being Administrators on their own workstations Use cable locks on portable computing devices that handle content (e.g., laptops, tablets, towers) when they are left unattended Intall remote-kill software on all portable computing devices that stonge	
System Security	DS-6.2 DS-6.3 DS-6.4 DS-6.5 DS-6.6	and on any device that connects to SAV/NAS systems. Update all anti-virus and anti-malware definitions daily, or more frequently. Scan all content for viruses and malware prior to ingest onto the content/production network. Perform scans as follows: Enable regular hill system virus and malware scanning on all workstations Enable regular hill system virus and malware scanning on all workstations Enable regular hill system virus and malware scanning on all workstations Enable regular bits strem virus and malware scans for servers and for systems connecting to a SAV/NAS implement a process to regularly update systems (e.g., file transfer systems, operating systems, databases, applications, network devices) with patchely duplest that remediate security virulenabilities. Prohibit users from being Administrators on their own workstations, unless required for software (e.g., ProTocis, Clipster and authoring software south as bit-mits General start Tochiba). Documentation from the software provider must explicitly state that administrative rights are required. Use cable locks on portable computing devices that handle content (e.g., tuptors, tablets, tower) when they use left unattended. Implement additional security controls for laptops and portable computing torage devices that romal areas intral remore kill storage on all uptopat/mobile devices that funde content to assiftware on all uptopat/mobile devices that funde content to allow remote wiping of hard drives sind other storage devices.	System Security	D5-6.0 D5-6.1 D5-6.2 D5-6.3 D5-6.4 D5-6.6 D5-6.6 D5-6.6	systems used for outputting content to physical media Install anti-virus offware on all workstations and servers Update anti-virus definitions daily Scan life baded content for viruses prior to ingest onto the content/production network Performing virus scans as follows: • nable regular hisystem virus scanning on all workstations • nable flui system virus scanns for servers, where applicable (e.g., non- SAV systems) Insplement a process to regularly update systems (e.g., file transfer systems, operating systems, databases, applicables (e.g., non- SAV systems) Insplement a process to regularly update systems (e.g., file transfer systems, operating systems, databases, applicables, network devices) Prohibit users from being Administrators on their own workstations Use cable locks on portable computing devices that handle content (e.g., laptops, tablets, towers) when they are left unattended Intall remote-kill software on all portable computing devices that stonge	
System Security	DS-6.2 DS-6.3 DS-6.4 DS-6.5 DS-6.6 DS-6.7	and on any device that connects to SAV/NAS systems. Update all anti-virus and anti-malware definitions daily, or more frequently. Scan all content for viruses and malware prior to ingest onto the content/production network. Perform scans as follows: - Enable regular hills system virus and malware scanning on all workstation - Snable regular hills system virus and malware scanning on all workstation - Snable regular hills system virus and malware scanning on all workstation - Snable regular hills system virus and malware scans for servers and for systems complement a process to regulary update systems (e.g., life transfer systems, operaning systems, database, spolications, retwork derice) with parchev/updates that remediate socurity vulnerabilities. Prohibit users from being Administrators on their own workstations, unless required for software (e.g., Procio, Clipster and autoring software such as Biu-Print, Scenarist and Toshiba). Documentation from the software provider must explicitly start that administrative rights are required. Use cable locks on portable computing devices that handle content (e.g., laptoph, tablets, towers) short they are left unstended. Implement additional scenarity controls for laptops and portable computing storage devices. that and incontent sill software on all potpolymobil devices that administration source to sensitive information protable computing storage devices. Install renome-kill software on all potpolymobil devices that administration to display storage of devices in laptopy. The devices that administration to allow remote wiping of hard drives and other storage devices.	System Security	D5-6.0 D5-6.1 D5-6.2 D5-6.3 D5-6.4 D5-6.6 D5-6.6 D5-6.6	systems used for outputting content to physical media Install anti-virus software on all workstations and servers Update anti-virus definitions daily Scan file-based content for viruses prior to ingest onto the content/production network. Performing virus scans as follows: I make regular full system virus scanning on all workstations I make regular full system virus scanning on all workstations I make regular full system virus scans for servers, where applicable (e.g., non- SAV systems) Implement a process to regularly update systems (e.g., life transfer systems, operating systems, database, applicablos, encloved devices) with patches/updates that remediate security vulnerabilities Prohibit users from being Administrators on their own workstations Use cable locks on portable computing devices that handle content (e.g., laptops, tablets, towers) when they are left unattended install remote-kill isoftware on all portable computing devices that handle content to allow remote wiping of hard drives and other storage devices Restrict software installation privileges to approved users Inglement security baselines and standards to configure systems (e.g., Restricts offware installation privileges to approved users	
System Security	DS-6.2 DS-6.3 DS-6.4 DS-6.5 DS-6.6 DS-6.7 DS-6.7	and on any device that connects to SAN/NAS systems. Update all anti-virus and anti-malware definitions daily, or more frequently. Scan all content for viruses and malware prior to ingest onto the content/production network. Perform scans as follows: A subject of the system virus and malware scanning on all workstation and subjects virus and malware scans for servers and for systems complement and system virus and malware scans for servers and for systems complements a packets to regularly update systems (e.g., life transfer complements) a packets to regularly update systems (e.g., life transfer systems, operaning systems, disabases, applications, entervirus exploring a packets to regularly update systems (e.g., life transfer systems, operaning systems, disabases, applications, entervirus exploring a society of the system virus and Toshiba). Documentation from is oftware required. Life cable locks on portable computing devices that handlie content (e.g., laptops, tablets, towers) when they are left unstrended. Implement additional security controls for laptops and portable computing storage devices that toraids content or sensitive information relating to client projects. Enzyst all haptops. Use hardware-encrypted stoppiory/molid devices that toraids. Contents to allow remote wiping of hard drives and other storage devices. The management. Implement activity balaelises and storadis to configure systems (e.g., laptops, workstations, servers, SAN/NAS) that are set up internally.	System Security	05-6.0 05-6.1 05-6.3 05-6.4 05-6.5 05-6.5 05-6.6 05-6.7	systems used for outputting content to physical media Install anti-virus offware on all workstations and servers Update anti-virus definitions daily Scan life based content for viruses prior to ingest onto the content/production network Performing virus scans as follows: • Enable reguler flay stems (viruse) prior to ingest onto the content/production network Performing virus scans for servers, where applicable (e.g., non- SAN systems) Implement a process to regularly update systems (e.g., file transfer systems, operating systems, databaset, applicable (e.g., non- SAN systems) Implement a process to regularly update systems (e.g., file transfer systems, operating systems, databaset, applications, network devices) Into active/updates that remediate accurity unlenabilities Prohibit users from being Administrators on their own workstations Use cable locks on portable computing devices that handle content (e.g., laptops, tablets, towers) when they are left unattended install remote-kill software on al portable computing devices that handle content to allow remote wiping of hard drives and other storage devices Restrict software installation privileges to approved users implement security baselines and standards to configure systems (e.g., laptops, workstations, server) (that are set up internally	
System Security	DS-6.2 DS-6.3 DS-6.4 DS-6.5 DS-6.6 DS-6.6 DS-6.7 DS-6.8 DS-6.9 DS-6.10	and on any device that connects to SAV/NAS systems. Update all anti-virus and anti-malware definitions daily, or more frequently. Scan all content for viruses and malware prior to ingest onto the content/production network. Perform scans as follows: E-fable regular hill system virus and malware scanning on all workstations E-fable regular hill system virus and malware scanning on all workstations E-fable regular hill system virus and malware scanning on all workstations E-fable regular hill system virus and malware scans for servers and for systems Connecting as SAV/NAS systems, operanging systems, drahbase, spollcations, enhow devices] with patches/updates that remediate socurity vulnerabilities. Prohibit users from being Administrators on their own workstations, unless required for must explicitly state that administrations software such as Biu-Print, Scenarist and Toshiba). Documentation from the software provider must explicitly state that administrations refugated. Use cable locks on portable computing devices that handle content (e.g., laptops, tablets, tovers) when they are left unstrended. Implement additional security controls for laptops and portable computing storage devices. Into atmal remote All storators on a laptop/mobile devices that handle content to estative information relating to client projects. Enzry all laptops. Use hardware encrypted partiale computing torage devices. Into atmale metake all singer of had drives and obtained to content to management. Implement scattify batelines and stratadits to configure systems (e.g., laptops, workstations, servers, SAN/NAS) that are set up internally. Unnecessary services and applications should be uninstalled from content transfer serves.	System Security	D5-6.0 D5-6.1 D5-6.2 D5-6.3 D5-6.4 D5-6.6 D5-6.6 D5-6.6	systems used for outputting content to physical media Install anti-virus software on all workstations and servers Update anti-virus definitions daily Scan file-based content for viruses prior to ingest onto the content/production network. Performing virus scans as follows: I make regular full system virus scanning on all workstations I make regular full system virus scanning on all workstations I make regular full system virus scans for servers, where applicable (e.g., non- SAV systems) Implement a process to regularly update systems (e.g., life transfer systems, operating systems, database, applicablos, encloved devices) with patches/updates that remediate security vulnerabilities Prohibit users from being Administrators on their own workstations Use cable locks on portable computing devices that handle content (e.g., laptops, tablets, towers) when they are left unattended install remote-kill isoftware on all portable computing devices that handle content to allow remote wiping of hard drives and other storage devices Restrict software installation privileges to approved users Inglement security baselines and standards to configure systems (e.g., Restricts offware installation privileges to approved users	
System Security	DS-6.2 DS-6.3 DS-6.4 DS-6.5 DS-6.6 DS-6.7 DS-6.7	and on any device that connects to SAV/NAS systems. Update all anti-virus and anti-malware definitions daily, or more frequently. Scan all content for viruses and malware prior to ingest onto the content/production network. Perform scans as follows: Enable regular hill system virus and malware scanning on all workstations Enable regular hill system virus and malware scanning on all workstations Enable regular hill system virus and malware scanning on all workstations Enable full system virus and malware scans for servers and for systems connecting to a SAV/NAS thin particle Judgets that remediate security virunerabilities. Prohibit users from being Administrators on their own workstations, miles required for software (e.g., Protocis, Dispitar and authoring software soin a Bain-Print, Scenaris and Tohiba). Documentation from the software provider must explicitly state that administrative rights are regulated. Kick on portable computing devices that handle content (e.g., tupiose, tablets, towers) when they are left unattended. Implement additional security controls for laptops and portable computing storage devices that contail ensure information mating to client projects. Encrypt all laptops. Use hardware encrypted protable computing storage devices. Intail remote-kill storage of hard drives and other storage devices. Intail remote-kill storage of hard drives and other storage devices. Intail remote-kill storage of hard drives and other storage devices. Intail remote-kill storage of hard drives and other storage devices. Intail remote-kill storage of hard drives and other storage devices. Intail remote-kill storage of hard drives and other storage devices. Intail remote-kill storage of hard hard drives and other storage devices. Intail remote-kill storage of hard hard drives and other storage devices. Intail remote-kill storage of hard hard drives and other storage devices. Intail remote-kill storage of hard hard drives and other storage devices. Intail remote-kill storage of ha	System Security	05-6.0 05-6.1 05-6.3 05-6.4 05-6.5 05-6.5 05-6.6 05-6.7	systems used for outputting content to physical media Install anti-virus software on all workstations and servers Update anti-virus definitions daily Scan file-based content for viruses prior to ingest onto the content/production network. Performing virus cans as follows: • Enable regular full system virus scann from an all workstations • Enable regular full system virus scann for one all workstations • Enable regular full system virus scann for evens, where applicable (e.g., non- SM system) Implement a process to regularly update systems (e.g., file transfer systems, operating systems, databases, applications, network devices) with patchet/updates that remediate security vulnerabilities Prohibit users from being Administrators on their own workstations Use cable locks on portable computing devices that handle content (e.g., laptops, tablets, towers) when they are left unattended install remote-kill software on all portable computing devices that handle content to allow remote wiping of hard drives and other storage devices Restrict software installation privileges to approved users implement security baselines and standards to configure systems (e.g., laptops, workstatile from	
System Security	D5-6.2 D5-6.3 D5-6.4 D5-6.5 D5-6.5 D5-6.6 D5-6.7 D5-6.8 D5-6.9 D5-6.10 D5-6.11	and on any device that connects to SAV/NAS systems. Update all anti-virus and anti-malware definitions daily, or more frequently. Scan all content for viruses and malware prior to ingest onto the content/production network. Perform scans as follows: Enable regular hill system virus and malware scanning on all workstations Enable regular hill system virus and malware scanning on all workstations Enable regular hill system virus and malware scanning on all workstations Enable regular bits systems, classifications, network devices) with particle/updates that remediate security virunerabilities. Prohibit users from being Administrators on their own workstations, unless regulered for software (e.g., Protocls, Dispitar and authoring software south as Burrint, Scenaris and Tochhala). Documentation from the software provider must explicitly state that damining states, and exists, toxens) when they are left unstended. Use cable locks on portable computing devices the thandle content (e.g., tuptoss, tablets, toxens) when they are left unstended. Implement additional security controls for laptops and portable computing storage devices. Into contail remoter visits information match required devices that contail escurate information mon- taing to client projects. Encrypt all laptops. Use hardware encrypted protable computing devices that frandet escure to allow remote wiping of hard drives and other storage devices. Intel monale information and laptops, workstream escurity baselines and standards to configure systems (e.g., laptops, workstream escurity baselines and standards to to allow remote wiping of hard drives and applications should be uninstated from content transfer servers.	System Security	05-6.0 05-6.1 05-6.3 05-6.4 05-6.5 05-6.5 05-6.6 05-6.7	systems used for outputting content to physical media Install anti-virus software on all workstations and servers Update anti-virus definitions daily Scan file-based content for viruses prior to ingest onto the content/production network. Performing virus cans as follows: • Enable regular full system virus scann from an all workstations • Enable regular full system virus scann for one all workstations • Enable regular full system virus scann for evens, where applicable (e.g., non- SM system) Implement a process to regularly update systems (e.g., file transfer systems, operating systems, databases, applications, network devices) with patchet/updates that remediate security vulnerabilities Prohibit users from being Administrators on their own workstations Use cable locks on portable computing devices that handle content (e.g., laptops, tablets, towers) when they are left unattended install remote-kill software on all portable computing devices that handle content to allow remote wiping of hard drives and other storage devices Restrict software installation privileges to approved users implement security baselines and standards to configure systems (e.g., laptops, workstatile from	
System Security	D5-6.2 D5-6.3 D5-6.4 D5-6.5 D5-6.5 D5-6.6 D5-6.7 D5-6.8 D5-6.9 D5-6.10 D5-6.11	and on any device that connects to SAV/NAS systems. Update all anti-virus and anti-malware definitions daily, or more frequently. Scan all content for visuss and malware prior to ingest onto the content/production network. Perform stams as follow: • Enable regard indi system visus and malware scanning on all • Enable full system visus and malware scanning on all • Enable Automation systems, databases, applications, retwork devicely with patche/updates that remediate security vulnerabilities. Prolibit users from being Administrators on their own workstations, unless required for Software (e.g., Protoc), Clipster and automing software such as Bu-Print, Scenarist and Toshiba). Documentation form the software protocy. Toshiba that and the software protocy and the software interprotect and toshiba that and exonter rights are required. Loc cable locs on portable computing devices that handle content (e.g., hyptops, Jubets, towers) when they are list unattended. Implement additional security controls for spops and portable computing storage devices. Install remote-ill software on all stoptowing storage devices. Install remote-ill software on all stoptowing storage devices. Install remote-ill software on laptops/mobile devices. Install remote-ill software on all stoptowing storage devices. Install remote-ill software on all stoptowing storage devices. Install remote-ill software on all stoptowing of the storage devices. Install remote-ill software on all stoptowing storage devices. Installer on the storage of the stoptowing storage and system components	System Security	05-6.0 05-6.1 05-6.3 05-6.4 05-6.5 05-6.5 05-6.6 05-6.7	systems used for outputting content to physical media Install anti-virus offware on all workstations and servers Update anti-virus definitions daily Scan file-based content for viruses prior to ingest onto the content/production network. Performing virus cans as follows: • Enable full system virus scanning on all workstations • Enable full system virus scanning on all workstations with patchet/updates that remediate security vulnerabilities prohibit users from being Administrators on their own workstations Use cable locks on portable computing devices that handle content (e.g., laptops, tablets, towers) when they are left unattended install remote-kill software on all portable computing devices that handle content to allow remote wiping of hard drives and other storage devices Restrict coftware installation privileges to approved users implement security baselines and standards to configure systems (e.g., laptops, workstations, servers) that are set up internally Unnecessing services and applications should be uninstalled from content transfer servers	documented network topology.
System Security	05-6.2 05-6.3 05-6.5 05-6.5 05-6.5 05-6.7 05-6.10 05-6.12	and on any device that connects to SAV/NAS systems. Update all anti-virus and anti-malware definitions daily, or more frequently. Scan all content for viruses and malware prior to ingest onto the content/spracticum network. Perform Status as follows: - Enable regular this system virus and malware scanning on all workstations - Enable regular this system virus and malware scanning on all workstations - Some child to system virus and malware scanning on all workstations - Some child to system virus and malware scanning on all workstations - Some child to system virus and malware scanning on all workstations - Some child to system virus and malware scanning on all workstations - Instance and the system virus applications, enterother with patches/updates that remediate security virinerabilities. - Prohibit users from being Administratoro on their own workstations, unless required for must egicity status that administrative rights are required. Lue cable looks on portable computing devices that handle content (e.g., laptoss, labels, towers) when they are left unstended. - Implement additionel security controls for splapos and portable computing storage devices. Incall ermode- will software on all storage devices that landle content to allow remote wiping of hard drives and other storage devices. - Restrict Software installation privileges to C management. - Implement additionels, servers, SAVIXSD that are stup internally. - Unnecessary services and applications should be uninstalled from content transfer servers. - Montain inventory of splaps and splating content prives servers. - Montain inventory of splaps and splates contents. - Montains inventory of splaps and	System Security	05-6.0 05-6.1 05-6.2 05-6.3 05-6.5 05-6.6 05-6.6 05-6.7 05-6.7	systems used for outputting content to physical media Install anti-virus software on all workstations and servers Update anti-virus definitions daily Scan file-based content for viruses prior to ingest onto the content/poduction networks in content/poduction networks in content production networks in content production networks in the second file system virus scans for servers, where applicable (e.g., non- SAN systems) implement a process to regularly update systems (e.g., file transfer systems, operating systems, databases, applications, network devices) with patchel/updates that remediate security vulnerabilities prohibit users from being Administrators on their own workstations Use cable locks on portable computing devices that handle content (e.g., laptops, tablets, towers) when they are left unattended install remote-kill software on all portable computing devices that handle content to allow remote wiping of hard drives and other storage devices Restrict software installation privileges to approved users implement security baselines and standards to configure systems (e.g., uptops, unstallations, serven) that are use up intermally unnecessary services and applications should be uninstalled from content transfer servers	documented network topology.
System Security	05-6.2 05-6.3 05-6.5 05-6.5 05-6.5 05-6.7 05-6.10 05-6.12	and on any device that connects to SAV/NAS systems. Update all anti-virus and anti-malware definitions daily, or more frequently. Scan all content for viruses and malware prior to injest onto the content/groupduction network. Perform scans as follows: E- Enable regular hill system virus and malware scanning on all workstations E- Enable regular hill system virus and malware scanning on all workstations E- Enable regular hill system virus and malware scans for servers and for systems connecting to a SAV/NOS implement a processor tregularly update systems (e.g., file transfer systems, operating system, classbase, spokcatons, network devices) with aptache/updates hart remediate security wirersoffices. Prohibit users from being Administrators on their own workstations, unless required for software (e.g., Proc)CL (Dister and autoring software souch as But-Print). Security and Tashibab, Documentation from the software proved must explicitly state that administrative regulared. Use cable locks on portable computing devices that handle content (e.g., laptos), tablets, towers) when they are left unitended. Implement additional security controls for laptosa and portable computing storage devices. Intal remote-Hall software on all laptos/mobile devices that handle content to sansitive on all laptos/mobile devices that handle is confliper systems (e.g., laptos, unclustions, servers, SAV/NAS) that are use uniternally. Unnecessary services and applications should be uninstalled from content transfer servers. Maintian an inventory of system and system components. Societtic transge are servers.	System Security	05-6.0 05-6.1 05-6.2 05-6.3 05-6.5 05-6.6 05-6.6 05-6.7 05-6.7	systems used for outputting content to physical media Install anti-virus offware on all workstations and servers Update anti-virus definitions daily Scan file-based content for viruses prior to ingest onto the content/poduction network is chable regular hill system virus scaning on all workstations - Enable regular hill system virus scaning on all workstations - Enable regular hill system virus scaning on all workstations - Enable regular hill system virus scaning for all workstations - Bable regular bits systems, databases, applicable (e.g., non- SN systems) Implement a process to regularly update systems (e.g., file transfer systems, operating systems, databases, applicables, network devices) hin patchefu/qubates that remediate security vulnerabilities - Prohibit users from being Administrators on their own workstations - Install enough the system security vulnerabilities - Prohibit users from being Administrators on their own workstations - Install enough the system security vulnerabilities - Install enough the system security security security security - aptrops, tablets, towers) when they are left unattended - Install enough the stallation privileges to approved users - Installer content to allow remote wiping of hard drives and other storage devices - Restrict software installation privileges to approved users - Inspective security baselines and standards to configure systems (e.g., - plotos, unstables, server) that are use us internally - Unnecestary services and applications should be uninstalled from content transfer servers	documented network topology.

The table block was created by AVGS to highlight the defaultation of the AP practices published in 2013 and the MPAA best practices published in 2015. • For any new control added to the 2015 MPAA best practices, see any rows highlighted in "green." • For any control set which had a slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "green." • For any control set which had a slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "green." • For any control set which had a slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "blue." • For any control set which had for the 2014 MPAA best practices, see controls were highlighted in "green."

	MP	AA Best Practices 2015		MP	AA Best Practices 2013	AWS comments on the differences between 2015 and 2013 version
Security Topic	No.	Best Practice	Security Topic	No.	Best Practice	
	DS-7.2	Assign unique credentials on a need-to-know basis using the principles		DS-7.2	Assign unique credentials on a need-to-know basis using the principles	
	DS-7.3	of least privilege. Rename the default administrator accounts and other default accounts		DS-7.3	of least privilege Rename the default administrator accounts and limit the use of these	
		and limit the use of these accounts to special situations that require			accounts to special situations that require these credentials (e.g.,	
		these credentials (e.g., operating system updates, patch installations, software updates).			operating system updates, patch installations, software updates)	
Account Management	DS-7.4	Segregate duties to ensure that individuals responsible for assigning	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			access to information systems are not themselves end users of those systems (i.e., personnel should not be able to assign access to	
		systems (i.e., personnel should not be able to assign access to themselves).			systems (i.e., personnel should not be able to assign access to themselves)	
	DS-7.5	Monitor and audit administrator and service account activities.		DS-7.5	Monitor and audit administrator and service account activities	
	DS-7.6	Implement a process to review user access for all information systems that handle content and remove any user accounts that no longer		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.			require access quarterly	
	DS-7.7 DS-7.8	Restrict user access to content on a per-project basis.		DS-7.7 DS-7.8	Review user access to content on a per-project basis	
	D3-7.8	Disable or remove local accounts on systems that handle content where technically feasible.		D3-7.8	Disable or remove local accounts on systems that handle content where technically feasible	
	DS-8.0	Enforce the use of unique usernames and passwords to access		DS-8.0	Enforce the use of unique usernames and passwords to access	2015 MPAA suggest the provider implement additional authentication
	DS-8.1	information systems. Enforce a strong password policy for gaining access to information		DS-8.1	information systems Enforce a strong password policy for gaining access to information	mechanisms, which would provide a layered authentication strategy.
		systems.			systems	
	DS-8.2	Implement two-factor authentication (e.g., username/password and hard token) for remote access (e.g., VPN) to the networks.		DS-8.2	Implement two-factor authentication (e.g., username/password and hard token) for remote access (e.g., VPN) to the networks.	
Authentication		hard token) for remote access (e.g., VPN) to the networks.	Authentication		nard token) for remote access (e.g., VPN) to the networks.	
	DS-8.3	Implement password-protected screensavers or screen-lock software for		DS-8.3	Implement password-protected screensavers or screen-lock software for	
	DS-8.4	servers and workstations. Consider implementing additional authentication mechanisms to			servers and workstations	
		provide a layered authentication strategy for WAN and LAN / Internal				
	DS-9.0	Network access.		DS-9.0		
	03-9.0	Implement real-time logging and reporting systems to record and report security events; gather the following information at a minimum:		03-9.0	Implement real-time logging and reporting systems to record and report security events; gather the following information at a minimum:	months. As well as, the requirement to manage the logs in a central
		When (time stamp)			When (time stamp)	repository.
		Where (source) Who (user name)			Where (source) Who (user name)	
		• What (content)			• What (content)	
	DS-9.1	Implement a server to manage the logs in a central repository (e.g.,		DS.S-9.0	Implement logging mechanisms on all systems used for:	
		syslog/log management server, Security Information and Event Management (SIEM) tool).			Key generation Key management	
		management (SIEM) tool).			Key management Vendor certificate management	
	DS-9.2	Configure logging systems to send automatic notifications when security events are detected in order to facilitate active response to incidents.		DS-9.1	Configure logging systems to send automatic notifications when security events are detected in order to facilitate active response to incidents	
	DS-9.3	Investigate any unusual activity reported by the logging and reporting		DS-9.2	Investigate any unusual activity reported by the logging and reporting	
	DS-9.4a	systems. Implement logging mechanisms on all systems used for the following:		DS-9.3	systems Review logs weekly	
		Key generation				
		Key management Vendor certificate management				
Logging and Monitoring		-	Logging and Monitoring			
	DS-9.4b	Review all logs weekly, and review all critical and high daily.		DS-9.4	Enable logging of internal and external content movement and transfers	
					and include the following information at a minimum: • Username	
					Timestamp	
					File name Source IP address	
					Destination IP address	
					Event (e.g., download, view)	
	DS-9.5	Enable logging of internal and external content movement and transfers		DS-9.5	Retain logs for at least 6 months	
		and include the following information at a minimum:				
		Username Timestamp				
		File name				
		Source IP address Destination IP address				
		Event (e.g., download, view)				
	DS-9.6 DS-9.7	Retain logs for at least one year.		DS-9.6 DS-9.7	Restrict log access to appropriate personnel	
	D3-9.7	Restrict log access to appropriate personnel.		D5-9.7	Send automatic notifications to the production coordinator(s) upon outbound content transmission	
	DS-10.0	Develop a BYOD (Bring Your Own Device) policy for mobile devices				2015 MPAA added this control set.
	DS-10.1	accessing or storing content. Develop a list of approved applications, application stores, and				
		application plugins/extensions for mobile devices accessing or storing				
	DS-10.2	content. Maintain an inventory of all mobile devices that access or store content.				
	03-10.2					
	DS-10.3	Require encryption either for the entire device or for areas of the device				
Mobile Security	DS-10.4	where content will be handled or stored. 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.				
	DS-10.6	Implement automatic locking of the device after 10 minutes of non-use.				
	DS-10.7	Manage all mobile device operating system patches and application				
		updates.				
	DS-10.8	Enforce password policies.				
	DS-10.9	Implement a system to perform backup and restoration of mobile devices.				
	DS-11.0	Ensure that security techniques (e.g., spoiling, invisible/visible		DS-10.0	Ensure that security techniques (e.g., spoiling, invisible/visible	2015 MPAA added controls around the encryption of content at rest and
		watermarking) are available for use and are applied when instructed.			watermarking) are available for use and are applied when instructed	in motion. Additionally, procedures around the storage of public and private keys.
	DS-11.1	Encrypt content on hard drives or encrypt entire hard drives using a		DS.S-10.0	Implement a process for key management that addresses the following:	
		minimum of AES 128-bit, or higher, encryption by either:			Approval and revocation of trusted devices Generation, renewal, and revocation of content keys	
		 File-based encryption: (i.e., encrypting the content itself) Drive-based encryption: (i.e., encrypting the hard drive) 			Generation, renewal, and revocation of content keys Internal and external distribution of content keys	
	DS-11 2	Send decryption keys or passwords using an out-of-band communication		DS-10.1	Encrypt content on hard drives using a minimum of AES 128-bit	
		protocol (i.e., not on the same storage media as the content itself).			encryption by either:	
					File-based encryption: (i.e., encrypting the content itself) Drive based encryption: (i.e., encrypting the bard doub)	
					 Drive-based encryption: (i.e., encrypting the hard drive) 	
	DS-11.3	Implement and document key management policies and procedures:		DS.S-10.1	Confirm that devices on the Trusted Devices List (TDL) are appropriate	
		 Use of encryption protocols for the protection of sensitive content or data, regardless of its location (e.g., servers, databases, workstations, 			based on rights owners' approval	
		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	Security Techniques/Advanced Security			
Security Techniques		 Segregate duties to separate key management from key usage Key storage procedures 	Techniques			
		Key storage procedures Key backup procedures				
	DS-11.4	Encrypt content at rest and in motion, including across virtual server		DS-10.2	Send decryption keys or passwords using an out-of-band communication	
		instances, using a minimum of AES 128-bit, or higher, encryption.			protocol (i.e., not on the same storage media as the content itself)	

The table below was created by AWS to highlight the delta between the MPAA best practices published in 2013 and the MPAA best practices published in 2013 and the MPAA best practices published in 2015. For any new control added to the 2015 MPAA best practices, see any rows highlighted in "green." For any control set which had a slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "green." For any control set which had a slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "blue." For any control set which had slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "blue." For any control set which has removed from the 2015 MPAA best practices, the controls were fulfighted in "green."

MPAA Best Practices 2015				MP.	APAA Best Practices 2013 AWS comments on the differences between 2015 and 2013 version		
Security Topic	No.	Best Practice	Security Topic	No.	Best Practice		
	DS-11.5	Store secret and private keys (not public keys) used to encrypt data/content in one or more of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data- encrypting key. Within a secure cryptographic device (e.g., host Security Module (HSM) or a hin Transaction Security (PTS) point of interaction device) o His at least two full-length key components or key shares, in accordance with a security industry accepted method		DS.S-10.2	Confirm the validity of content keys and ensure that expiration dates conform with client instructions		
	DS-11.6 DS-11.7	Confirm that devices on the Trusted Devices List (TDL) are appropriate based on rights owners' approval. Confirm the validity of content keys and ensure that expiration dates					
Content Tracking	DS-12.0 DS-12.1 DS-12.2 DS-12.3	conform to client instructions. Implement a digital content management system to provide detailed tracking of digital content. Readin adjutal content movement transaction logs for one year. Review logs from digital content management system periodically and investigate anomalies. Use client AKAK ("aliases") when applicable in digital asset tracking systems.				2015 MPAA added this control set.	
	DS-13.0 DS-13.1	Use only client-approved transfer systems that utilitie access controls, a minimum of AES 128-bit, or higher, encryption for content at rest and for content in motion and use strong authorization for content transfer assistes. Implement are acception process, where prior client approval must be obtained in writing, to address situations where encrypted transfer tools are not used.				2015 MPAA added this control set.	
Transfer Device Methodology	DS-14.0 DS-14.1 DS-14.2 DS-14.3 DS-14.4	Implement and use dedicated systems for content transfers. Separate content transfer systems from administrative and production networks. Place content transfer systems in a Demilitarized Zone (DMZ) and not in the content/production network. Remove content from content transfer devices/systems immediately after successful transmission/receipt. Send automatic notifications to the production coordinator(s) upon outbound content transmission.	Transfer Device Methodology	DS-12.2 DS-12.3	Implement and use dedicated systems for content transfers Segment systems dedicated to transfer files from systems that store or process content and from the on-production network Place content transfer systems in a Demiltanted Zone (DMZ) and not in the content/production network Remove content from content transfer devices immediately after successful transmission/receipt	2015 MPAA added a control around sending automatic notification for content transmition.	
Client Portal	DS-15.11	Restrict access to web portain which are used for transferring content, streaming content and key distribution to authorized users. Assign unique credentials (e.g., usemanne and password) to portal users and distribute credentials to clients accured to the stream users only was access to there on digital assets (i.e., client A stream users only was access to there on the DM2 and limit access to provide the web portal on addicated assers in the DM2 and limit access to provide the use of third-party production software/system/services mobility the use of third-party production software/system/services mobility the use of third-party production software/system/services advance. Use hTTPS and enforce use of a store credentials in plaintext. Set access to content on internal or external portals to expire automatically at predefined intervaix, where configurable. Fact for web application vulnerabilities quarterly and remediate any validated issues. Perform annual pertention testing of web applications and remediate any validated issues. Parking the testing of web applications and remediate any validated issues. Parking the testing of web applications and remediate any validated issues. Purblit transmission of content using email (including webmail). Review access to the client web portal latest quarterly.	Client Portal	DS-13.2 DS-13.3 DS-13.4 DS-13.5 DS-13.6 DS-13.7 DS-13.7 DS-13.8 DS-13.9 DS-13.10	Restrict access to web portals which are used for transferring content, streaming content and key distribution to authorized users Asign unique credentials (e.g., username and password) to portal users and distribute credentials to clients accurely finance users only was access to there on digital assets (i.e., client A musc the hard pocess to clients distribution to authorized users of the advectory of the distribution to authorized users and distribute credentials to clients accurely finance users only and postcore distribution of the advectory prohibit the use third-party production tracking coffware that is hosted on internet web server unless approved by client Use HTTPS and enforce use of a storing cipher suffe (e.g.,SSU3 or TLS VI) for the internal/acternal web portal automatically at predefined intervals, where configurable Test for web application vulnerabilities annually Allow only authorized personnel to request the establishment of a connection with the telecon service provider Phohibit transmission of content using e-mail (including webmail) from the actions of content using e-mail (including webmail) from the client postcore and on the persistion of content using e-mail (including webmail) from the client postcore and on the client web portal at least quarterly	2015 MPAA added a control around annual penetration testing of web applications.	
	DS-15.12	Review access to the client web portal at least quarterly.	Transfer Tools	DS-11.0 DS-11.1	Implement transfer tools that use access controls, a minimum of AES 128-bit encryption and strong authentication for content transfer sessions Implement an exception process, where client prior approval must be obtained in writing, to address situations where encrypted transfer tools are not used	2015 MPAA removed these controls.	