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

August 2016

verizon

digital media services

Content

1 Motion Picture of America Association (MPAA) Content Security Model

1.1 Purpose

In order to satisfy security and compliance requirements from content delivery network customers in the media industry, the deployment of solutions that meet industry-specific compliance requirements have been undertaken. This document is intended to provide information to assist Verizon Digital Media Services customers with evaluating these controls.

1.2 Scope

The MPAA specific controls and solutions described herein, apply to Verizon's content delivery network, Application Delivery Network, Verizon TRANSACT, Origin Storage and Verizon ROUTE; including the development and operational practices, security and monitoring of the network acceleration services with delivery regions in North America, South America, Europe and APAC.

1.3 MPAA Content Security Model Description

The 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.mpaa.org/content-security-program/

2 MPAA Control Implementation Descriptions

The table below documents Verizon Digital Media Services alignment with Motion Picture of America Association (MPAA) Content Security Model Guidelines released April 2, 2015.

No.	Security Topic	Best Practice	Verizon Implementation
MS-1.0	Executive Security Awareness /Oversight	Establish an information security management system that implements a control framework for information security approved by the business owner(s)/ senior management.	Verizon Digital Media Services (Verizon) has committed to the establishment, implementation, operation, monitoring, review, maintenance and improvement of an ISMS that complies with SOC 2, PCI DSS, and ISO/IEC 27001:2013 compliance for information security. Management review meetings (MRM) are held multiple times per year to ensure continuing suitability, adequacy and effectiveness of the ISMS and review security policies.
MS.S-1.1	Executive Security Awareness /Oversight	Review information security management policies and processes at least annually.	
MS.S-1.2	Executive Security Awareness /Oversight	Train and engage executive management/owner(s) on the business' responsibilities to protect content at least annually.	
MS.S-1.3	Executive Security Awareness /Oversight	Create an information security management group to establish and review information security management policies.	
MS-2.0	Risk Management	Develop a formal security risk assessment process focused on content workflows and sensitive assets to identify and prioritize risks of content theft and leakage that are relevant to the facility.	Verizon has a formally documented risk assessment and internal audit procedures that comply with ISO/IEC 27001:2013. In event of any findings, Corrective Action Reports are generated and a formal ISO Risk Assessment procedure is employed, as directed by accompanying policy. Risk Assessments are performed annually for SOC 2, PCI DSS, and ISO/IEC 27001:2013 compliance. External quarterly scans pertaining to PCI DSS requirements are performed by a PCI SSC Approved Scanning Vendor (ASV). Third-Party Vulnerability Testing is also performed. Clients are responsible for identifying high- security content and utilizing available security features accordingly. For example: token-based authentication allows customers to protect their content by the country, URL, IP address, protocol, or the referrer that linked to their content.
MS-2.1	Risk Management	Conduct an internal risk assessment annually and upon key workflow changes—based on, at a minimum, the MPAA Best Practice Common Guidelines and the applicable Supplemental Guidelines—and document and act upon identified risks.	

No.	Security Topic	Best Practice	Verizon Implementation
MS-3.0	Security Organization	Identify security key point(s) of contact and formally define roles and responsibilities for content and asset protection.	Verizon has identified, developed and implemented a means to identify the internal and external issues/parties that may impact the ability to meet and maintain the established ISMS. This is accomplished by identified the following: • Internal Parties • External Parties • Responsible and Accountable Roles Information Security is responsible for maintaining the above list and ensuring the ISMS Policy is updated, as changes are made to these affected personnel and parties. As parties are identified, their effect on the overall ISMS will be determined, documented and when appropriate, risks will be identified and treated. Verizon Information Security is responsible for identifying and maintaining all internal and external parties that may affect the ISMS, along with the requirements of these parties. The Security Operations team is hired by and reports to the Director of Security and is responsible for: • Leading the Information Security Forum • Prepare Information Security Forum security briefs • Maintain the ISMS • Establish and review the Security Risk Assessment • Select controls and risk treatment • Maintain the Statement of Applicability • Monitor ongoing compliance with security standards • Establish and maintain contacts with external security resources • Consult and advise on general information security issues • Lead the Incident Response Team • Record and resolve security incidents

No.	Security Topic	Best Practice	Verizon Implementation
MS-4.0	Policies and Procedures	Establish policies and procedures regarding asset and content security; policies should address the following topics, at a minimum: • Acceptable use (e.g., social networking, internet, phone, personal devices, mobile devices, etc.) • Asset and content classification and handling policies • Business continuity (backup, retention and restoration) • Change control and configuration management policy • Confidentiality policy • Digital recording devices (e.g., smart phones, digital cameras, camcorders) • Exception policy (e.g., process to document policy deviations) • Incident response policy • Mobile device policy • Network, internet and wireless policies • Password controls (e.g., password minimum length, screensavers) • Security policy • Visitor policy • Disciplinary/Sanction policy • Internal anonymous method to report piracy or mishandling of content (e.g., telephone hotline or email address)	Verizon has defined and implemented a series of objectives that support both the achievement of the ISMS and support the organization's strategic objectives. These security objectives are documented within the Information Security Objectives document that is defined and maintained by Security Operations. The objectives are reviewed and updated on at least an annual basis. The review of the security objectives are conducted and signed off by Security Operations Management and Executive Leadership. The ISMS Policy, Information Security Objectives, and supporting policies that affect the identified internal parties, external parties, and ISMS personnel are communicated and readily available to all parties. During annual security training and awareness programs, management ensures communication of the latest security policies, as well as written job descriptions for security management. Additionally, management is responsible for ensuring business associate agreements are current for employees and third parties. Human Resources in conjunction with the Director of Security have established a disciplinary process for violations to security requirements by employees. The language is noted within each security policy. Violation of policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution. Policies, procedures and relevant training programs are reviewed by independent external auditors during audits for our PCI DSS, and ISO/IEC 27001:2013 compliance.
MS.S-4.1	Policies and Procedures	Review and update security policies and procedures at least annually.	
MS-4.2	Policies and Procedures	Communicate and require sign-off from all company personnel (e.g., employees, temporary workers, interns) and third-party workers (e.g., contractors, freelancers, temp agencies) for all current policies, procedures, and/or client requirements.	

No.	Security Topic	Best Practice	Verizon Implementation
MS.S-4.3	Policies and Procedures	Develop and regularly update an awareness program about security policies and procedures and train company personnel and third-party workers upon hire and annually thereafter on those security policies and procedures, addressing the following areas at a minimum: • IT security policies and procedures • Content/asset security and handling in general and client-specific requirements • Security incident reporting and escalation • Disciplinary policy • Encryption and key management for all individuals who handle encrypted content • Asset disposal and destruction processes	Verizon has defined and implemented a series of objectives that support both the achievement of the ISMS and support the organization's strategic objectives. These security objectives are documented within the Information Security Objectives document that is defined and maintained by Security Operations. The objectives are reviewed and updated on at least an annual basis. The review of the security objectives are conducted and signed off by Security Operations Management and Executive Leadership. The ISMS Policy, Information Security Objectives, and supporting policies that affect the identified internal parties, external parties, and ISMS personnel are communicated and readily available to all parties. During annual security training and awareness programs, management ensures communication of the latest security policies, as well as written job descriptions for security management. Additionally, management is responsible for ensuring business associate agreements are current for employees and third parties. Human Resources in conjunction with the Director of Security have established a disciplinary process for violations to security requirements by employees. The language is noted within each security policy. Violation of policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution. Policies, procedures and relevant training programs are reviewed by independent external auditors during audits for our PCI DSS, and ISO/IEC 27001:2013 compliance.

No.	Security Topic	Best Practice	Verizon Implementation
MS-5.0	Incident Response	Establish a formal incident response plan that describes actions to be taken when a security incident is detected and reported.	Verizon maintains Security and Availability policies that address corporate governance, with regulatory considerations and environmental change response steps, a codified Incident Response framework, with action steps and guidelines for all departments for Security Incident Management processes. Customer SLAs define response times and update frequency. Security Incident reports are compiled as necessary upon the resolution of security incidents. Outstanding risks are also documented according to an ISO Internal Audit Procedure. All incidents reported in the CDN are tracked using a trouble ticketing system, and customers are informed of high-priority incidents (i.e., 1 - 3) via an RSS feed. Customers are also informed of service outages via a bulk e-mail notification and updates to the Verizon Network Status page to reflect service-impacting incidents. Incident management policy and procedures are reviewed by independent external auditors during audits for our PCI DSS, and ISO/IEC 27001:2013 compliance.
MS-5.1	Incident Response	Identify the security incident response team who will be responsible for detecting, analyzing, and remediating security incidents.	
MS-5.2	Incident Response	Establish a security incident reporting process for individuals to report detected incidents to the security incident response team.	
MS-5.3	Incident Response	Communicate incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client assets), and conduct a post-mortem meeting with management and client.	
MS-6.0	Business Continuity & Disaster Recovery	Establish a formal plan that describes actions to be taken to ensure business continuity.	The Verizon Digital Media Services global content delivery network is architected with full resiliency, redundancy and high availability in mind. Every aspect of the CDN is monitored for performance and problem identification. We incorporate business continuity and disaster recovery capabilities into all of our primary CDN offerings. Our platforms are monitored using a proprietary algorithm for determining capacity, performance, and security events. The CDN is monitored on a 24 x 7 x 365 basis by the Verizon Digital Media Services Network Operations Center (NOC). The NOC personnel have both standard and proprietary tools which focus on all aspects of CDN operation. When the CDN shows any alarms, the NOC has established procedures to troubleshoot the problem and to escalate to Tier 2 or higher levels in order to find and fix the root cause of the alarm. All incidents reported in the CDN are tracked using our current trouble ticketing system.
MS-6.1	Business Continuity & Disaster Recovery	Identify the business continuity team who will be responsible for detecting, analyzing and remediating continuity incidents.	

No.	Security Topic	Best Practice	Verizon Implementation
MS-7.0	Change Control & Configuration Management	Establish policies and procedures to ensure new data, applications, network, and systems components have been pre-approved by business leadership.	Verizon Digital Media Services has enacted an ITIL change management process for controlling the lifecycle of all changes. The goal of the change management process is to enable the introduction of beneficial changes without impact to the integrity or availability of Verizon Digital Media Services systems and services. Verizon Digital Media Services change management: • Insures the integrity and security of Verizon Digital Media Services content delivery services • Provides operational consistency • Provides governance of the approval process based on risk and urgency • Measures and provides metrics around changes and change management • Allows for identification and resolution for incidents and problems • Provides a central point for notification of changes
MS-8.0	Workflow	Document workflows tracking content and authorization checkpoints. Include the following processes for both physical and digital content: • Delivery (receipt/return) • Ingest • Movement • Storage • Removal/destruction	Content workflows for ingest, storage, delivery and removal are documented in Verizon Digital Media Services CDN Data Flow diagrams. Customers are responsible for utilizing suitable security or enabling security features for the entire lifecycle of their content. The effectiveness of key controls are assessed during the internal audit and risk assessment process. In event of any findings, Corrective Action Reports are generated and a formal ISO Risk Assessment procedure is employed, as directed by accompanying policy. Controls are reviewed annualy to identify and document changes to the process.
MS-8.1	Workflow	Update the workflow when there are changes to the process, and review the workflow process at least annually to identify changes.	
MS-9.0	Segregation of Duties	Segregate duties within the content workflow. Implement and document compensating controls where segregation is not practical.	Segregated duties exist within the content workflow for encryption key custodians, developers and support personnel. The network environment has been designed to segment production, development and staging environments with VLANs and ACLs. This is managed by the NOC and System Operations.

No.	Security Topic	Best Practice	Verizon Implementation
MS-10.0	Background Checks	Perform background screening checks on all company personnel and third-party workers.	It is the policy of Verizon to perform pre-employment background checks on all employees and any contractors that will have access to sensitive materials. In addition, if an employee changes positions in the Company, any additional required background checks for that position, which have not previously been performed, will be performed. The purpose of performing the checks is to determine and/or confirm, within appropriate legal and professional limits, a candidate's qualifications and suitability for the particular position for which they are being considered.
MS-11.0	Confidentiality Agreements	Require all company personnel to sign a confidentiality agreement (e.g., non-disclosure) upon hire and annually thereafter, that includes requirements for handling and protecting content.	Confidentiality agreements are signed by every employee, contractor and vendor prior to gaining access to the facilities and/or information about Verizon. The New Horizons' Policy and Verizon Network Access Control Policy address removing credentials and access rights of former employees, in a timely fashion, role-based access mechanisms within Active Directory and limited scope of access to only necessary systems. In event of employee termination, a codified checklist is followed to ensure permission controls and system access are adjusted accordingly.
MS-11.1	Confidentiality Agreements	Require all company personnel to return all content and client information in their possession upon termination of their employment or contract.	

No.	Security Topic	Best Practice	Verizon Implementation
MS-12.0	Third-party Use and Screening	Require all third-party workers (e.g., freelancers) who handle content to sign confidentiality agreements (e.g., non-disclosure) upon engagement.	Confidentiality agreements are signed by every employee, contractor and vendor prior to gaining access to the facilities and/or information about Verizon. All vendors are subject to a formalized new vendor certification and due diligence process. Verizon reviews third-party agreements for security controls and independent security audits of the various locations where content servers are hosted. Depending on the vendor providing these services, and the location where our servers are physically located, these locations typically include SAS70 type 2, SSAE16 type 1 and 2, or ISO/IEC 27001:2013 certification. The use of these locations is communicated to clients in the SSAE16 report and in the Security overview documentation. New Horizons' Policy and Verizon Network Access Control Policy address removing credentials and access rights of former employees, in a timely fashion, role-based access mechanisms within Active Directory and limited scope of access to only necessary systems. In event of employee termination, a codified checklist is followed to ensure permission controls and system access are adjusted accordingly. The checklist also ensures the return of company assets and data. The Secure Packaging, Delivery and Repurposing Procedure requires the removal, data wipe and destruction processes for assets that are to be re-purposed or decommissioned.
MS-12.1	Third-party Use and Screening	Require all third-party workers to return all content and client information in their possession upon termination of their contract.	
MS-12.2	Third-party Use and Screening	Include security requirements in third-party contracts.	
MS-12.3	Third-party Use and Screening	Implement a process to reclaim content when terminating relationships.	
MS-12.4	Third-party Use and Screening	Require third-party workers to be bonded and insured where appropriate (e.g., courier service).	
MS-12.5	Third-party Use and Screening	Restrict third-party access to content/production areas unless required for their job function.	
MS-12.6	Third-party Use and Screening	Notify clients if subcontractors are used to handle content or work is offloaded to another company.	

No.	Security Topic	Best Practice	Verizon Implementation
PS-1.0	Entry/Exit Points	Secure all entry/exit points of the facility at all times, including loading dock doors and windows.	Verizon requires badge access into all entry points with the HQ facility in Playa Vista, California. In addition, all visitors are required to be checked in by the receptionist, given a visitor badge and sign in. PoP physical security is managed by the PoP itself and Security Operations, upon contract signing, verifies that the physical security meets PCI DSS requirements. Verizon operating practice, existing procedures, and enforced policies, require: • Escorted access or no access in sensitive areas. • Physical Security protocols in data centers and where points of presence mandate. • Badging of employees in all areas, and a corporate culture that encourages accountability of all employees to challenge un-credentialed personnel in any area. Physical access to information resources is controlled using access cards and PINs to identify, authenticate and monitor all admittance attempts. Computer premises are safeguarded against unlawful and unauthorized physical intrusion. Verizon personnel are encouraged to challenge strangers on premises. Personnel authorized to enter secured area must escort personnel without an appropriate security clearance. When un-cleared personnel are present in these areas, sensitive information is protected from observation, disclosure, or removal. Physical Security controls are reviewed by independent external auditors during audits for our SOC 2, PCI DSS, and ISO/IEC 27001:2013 compliance.
PS-1.1	Entry/Exit Points	Control access to areas where content is handled by segregating the content area from other facility areas (e.g., administrative offices, waiting rooms, loading docks, courier pickup and drop-off areas, replication and mastering).	
PS-1.2	Entry/Exit Points	Control access where there are collocated businesses in a facility, which includes but is not limited to the following: • Segregating work areas • Implementing access-controlled entrances and exits that can be segmented per business unit • Logging and monitoring of all entrances and exits within facility • All tenants within the facility must be reported to client prior to engagement	

No.	Security Topic	Best Practice	Verizon Implementation
PS-2.0	Visitor Entry/Exit	Maintain a detailed visitors' log and include the following: • Name • Company • Time in/time out • Person/people visited • Signature of visitor • Badge number assigned	Verizon requires badge access into all entry points with the HQ facility in Playa Vista, California. In addition, all visitors are required to be checked in by the receptionist, given a visitor badge and sign in. PoP physical security is managed by the PoP itself and Security Operations, upon contract signing, verifies that the physical security meets PCI requirements. Verizon operating practice, existing procedures, and enforced policies, require: • Escorted access or no access in sensitive areas. • Physical Security protocols in data centers and where points of presence mandate. • Badging of employees in all areas, and a corporate culture that encourages accountability of all employees to challenge un-credentialed personnel in any area. Physical Security controls are reviewed by independent external auditors during audits for our SOC 2, PCI DSS, and ISO/IEC 27001:2013 compliance.
PS-2.1	Visitor Entry/Exit	Assign an identification badge or sticker which must be visible at all times, to each visitor and collect badges upon exit.	
PS-2.2	Visitor Entry/Exit	Do not provide visitors with key card access to content/ production areas.	
PS-2.3	Visitor Entry/Exit	Require visitors to be escorted by authorized employees while on-site, or in content/ production areas.	
PS-3.0	Identification	Provide company personnel and long-term third-party workers (e.g., janitorial) with a photo identification badge that is required to be visible at all times.	All company personnel and long-term third-party workers are issued photo identification that is validated and required to be visible at all times.

No.	Security Topic	Best Practice	Verizon Implementation
PS-4.0	Perimeter Security	Implement perimeter security controls that address risks that the facility may be exposed to as identified by the organization's risk assessment.	Sites are chosen to locate computer systems and to store data (including remote locations) are suitably protected from physical intrusion, theft, fire, flood, or excessive ambient temperature, humidity, electromagnetic disturbance and other hazards, as well as safe for Verizon personnel and visitors. Physical and environmental controls of our data centers are the responsibility of third-party data center vendors. Verizon requires badge access into all entry points with the HQ facility in Playa Vista, California. In addition, all visitors are required to be checked in by the receptionist, given a visitor badge and sign in. PoP physical security is managed by the PoP itself and Security Operations, upon contract signing, verifies that the physical security meets PCI requirements. Verizon operating practice, existing procedures, and enforced policies, require: • Escorted access or no access in sensitive areas. • Physical Security protocols in data centers and where points of presence mandate. • Badging of employees in all areas, and a corporate culture that encourages accountability of all employees to challenge un-credentialed personnel in any area. Physical access to information resources is controlled using access cards and PINs to identify, authenticate and monitor all admittance attempts. Computer premises are safeguarded against unlawful and unauthorized physical intrusion. Verizon personnel are encouraged to challenge strangers on premises. Personnel authorized to enter secured area must escort personnel without an appropriate security clearance. When un-cleared personnel are present in these areas, sensitive information is protected from observation, disclosure, or removal. Physical Security controls are reviewed by independent external auditors during audits for our SOC 2, PCI DSS, and ISO/IEC 27001:2013 compliance.
PS-4.1	Perimeter Security	Place security guards at perimeter entrances and non- emergency entry/exit points.	
PS-4.2	Perimeter Security	Implement a daily security patrol process with a randomized schedule and document the patrol results in a log.	
PS-4.3	Perimeter Security	Lock perimeter gates at all times.	

No.	Security Topic	Best Practice	Verizon Implementation
PS-5.0	Alarms	Install a centralized, audible alarm system that covers all entry/exit points (including emergency exits), windows, loading docks, fire escapes, and restricted areas (e.g., vault, server/machine room, etc.).	Physical and environmental controls of our data centers are the responsibility of third-party data center vendors. PoP physical security is managed by the PoP itself and Security Operations, upon contract signing, verifies that the physical security meets PCI requirements. Computer premises are safeguarded against unlawful and unauthorized physical intrusion. Physical Security controls are reviewed by independent external auditors during audits for our SOC 2, PCI DSS, and ISO/IEC 27001:2013 compliance.
PS-5.1	Alarms	Install and effectively position motion detectors in restricted areas (e.g., vault, server/machine room) and configure them to alert the appropriate security and other personnel (e.g., project managers, producer, head of editorial, incident response team, etc.).	
PS-5.2	Alarms	Install door prop alarms in restricted areas (e.g., vault, server, machine rooms) to notify when sensitive entry/exit points are open for longer than a pre-determined period of time (e.g., 60 seconds).	
PS-5.3	Alarms	Configure alarms to provide escalation notifications directly to the personnel in charge of security and other personnel (e.g., project managers, producer, head of editorial, incident response team, etc.).	
PS-5.4	Alarms	Assign unique arm and disarm codes to each person that requires access to the alarm system and restrict access to all other personnel.	
PS-5.5	Alarms	Review the list of users who can arm and disarm alarm systems quarterly, or upon change of personnel.	
PS-5.6	Alarms	Test the alarm system quarterly.	
PS-5.7	Alarms	Implement fire safety measures so that in the event of a power outage, fire doors fail open, and all others fail shut to prevent unauthorized access.	

No.	Security Topic	Best Practice	Verizon Implementation
PS-6.0	Authorization	Document and implement a process to manage facility access and keep records of any changes to access rights.	Documented procedures are followed for granting facility access for employees and remote hands contractors to production data centers. Verizon performs periodic data center access reviews to determine if key card security permissions are appropriate. Physical Security controls are reviewed by independent external auditors during audits for our SOC 2, PCI DSS, and ISO/IEC 27001:2013 compliance.
PS-6.1	Authorization	Document and implement a process to manage facility access and keep records of any changes to access rights.	
PS-6.1	Authorization	Restrict access to production systems to authorized personnel only.	
PS-6.2	Authorization	Review access to restricted areas (e.g., vault, server/machine room) quarterly and when the roles or employment status of company personnel and/or third-party workers are changed.	

No.	Security Topic	Best Practice	Verizon Implementation
PS-7.0	Electronic Access	Implement electronic access throughout the facility to cover all entry/exit points and all areas where content is stored, transmitted, or processed.	Physical access to information resources is controlled using access cards and PINs to identify, authenticate and monitor all admittance attempts. Computer premises are safeguarded against unlawful and unauthorized physical intrusion. Verizon personnel are encouraged to challenge strangers on premises. Personnel authorized to enter secured area must escort personnel without an appropriate security clearance. When un-cleared personnel are present in these areas, sensitive information is protected from observation, disclosure, or removal. Physical Security controls are reviewed by independent external auditors during audits for our SOC 2, PCI DSS, and ISO/IEC 27001:2013 compliance. Controls related to replication and mastering are not applicable.
PS.S-7.0	Electronic Access	Establish separate rooms for replication and for mastering	
PS-7.1	Electronic Access	Restrict electronic access system administration to appropriate personnel.	
PS-7.2	Electronic Access	Store card stock and electronic access devices (e.g., keycards, key fobs) in a locked cabinet and ensure electronic access devices remain disabled prior to being assigned to personnel. Store unassigned electronic access devices (e.g., keycards, key fobs) in a locked cabinet and ensure these remain disabled prior to being assigned to personnel.	
PS-7.3	Electronic Access	Disable lost electronic access devices (e.g., keycards, key fobs) in the system before issuing a new electronic access device.	
PS-7.4	Electronic Access	Issue third-party access electronic access devices with a set expiration date (e.g., 90 days) based on an approved timeframe.	
PS-8.0	Keys	Limit the distribution of master keys and / or keys to restricted areas to authorized personnel only (e.g., owner, facilities management).	Physical and environmental controls of our data centers are the responsibility of third-party data center vendors. PoP physical security is managed by the PoP itself and Security Operations, upon contract signing, verifies that the physical security meets PCI requirements. Computer premises are safeguarded against unlawful and unauthorized physical intrusion. Physical Security controls are reviewed by independent external auditors during audits for our SOC 2, PCI DSS, and ISO/IEC 27001:2013 compliance.
PS-8.1	Keys	Implement a check-in/check-out process to track and monitor the distribution of master keys and/or keys to restricted areas.	
PS-8.2	Keys	Use keys that can only be copied by a specific locksmith for exterior entry/exit points.	
PS-8.3	Keys	Inventory master keys and keys to restricted areas, including facility entry/exit points, quarterly.	
PS-8.4	Keys	Obtain all keys from terminated employees/third-parties or those who no longer need the access.	
PS-8.5	Keys	Implement electronic access control or rekey entire facility when master or sub-master keys are lost or missing.	

No.	Security Topic	Best Practice	Verizon Implementation
PS-9.0	Cameras	Install a CCTV system that records all facility entry/exit points and restricted areas (e.g., server/ machine room, etc.).	Physical and environmental controls of our data centers are the responsibility of third-party data center vendors. PoP physical security is managed by the PoP itself and Security Operations, upon contract signing, verifies that the physical security meets PCI requirements. Computer premises are safeguarded against unlawful and unauthorized physical intrusion. Physical Security controls are reviewed by independent external auditors during audits for our SOC 2, PCI DSS, and ISO/IEC 27001:2013 compliance.
PS-9.1	Cameras	Review camera positioning and recordings to ensure adequate coverage, function, image quality, lighting conditions and frame rate of surveillance footage at least daily.	
PS-9.2	Cameras	Restrict physical and logical access to the CCTV console and to CCTV equipment (e.g., DVRs) to personnel responsible for administering/monitoring the system.	
PS-9.3	Cameras	Ensure that camera footage includes an accurate date and time-stamp and retain CCTV surveillance footage and electronic access logs for at least 90 days, or the maximum time allowed by law, in a secure location.	
PS-9.4	Cameras	Designate an employee or group of employees to monitor surveillance footage during operating hours and immediately investigate detected security incidents.	

No.	Security Topic	Best Practice	Verizon Implementation
PS-10.0	Logging and Monitoring	Log and review electronic access to restricted areas for suspicious events, at least weekly.	Security Operations and the NOC directly control and manage the log ingestion from all systems. The logs are sent into aggregators that prevent the logs from being altered in any way. Security and Audit logs are enabled and pushed out either via GPO or directly configured locally on systems. Automated alerts are created for security events and reviewed daily by security analysts. Controls related to replication and mastering are not applicable. Verizon Security and Availability policies and procedures address the following: • A codified Incident Response framework, with action steps. • Guidelines for all departments for Security Incident Management processes. Security Incident reports are compiled as necessary upon the resolution of security incidents. Outstanding risks are also documented according to an ISO Internal Audit Procedure. Physical Security controls are reviewed by independent external auditors during audits for our SOC 2, PCI DSS, and ISO/IEC 27001:2013 compliance.
PS-10.1	Logging and Monitoring	Log and review electronic access, at least daily, for the following areas: • Masters/stampers vault • Pre-mastering • Server/machine room • Scrap room • High-security cages	
PS-10.2	Logging and Monitoring	Investigate suspicious electronic access activities that are detected.	
PS-10.3	Logging and Monitoring	Maintain an ongoing log of all confirmed electronic access incidents and include documentation of any follow-up activities that were taken.	

No.	Security Topic	Best Practice	Verizon Implementation
PS-11.0	Searches	Establish a policy, as permitted by local laws, which allows security to randomly search persons, bags, packages, and personal items for client content.	Not applicable: Verizon does not handle any physical assets for content under MPAA security constraints. Content is instead ingested electronically and pre-encrypted with security features deemed appropriate by the customer. Physical Searches for previously DRM secured assets are not required. Physical Security controls are reviewed by independent external auditors during audits for our SOC 2, PCI DSS, and ISO/IEC 27001:2013 compliance.
PS.S-11.1	Searches	Implement an exit search process that is applicable to all facility personnel and visitors, including: • Removal of all outer coats, hats, and belts for inspection • Removal of all pocket contents • Performance of a self pat-down with the supervision of security • Thorough inspection of all bags • Inspection of laptops' CD/DVD tray • Scanning of individuals with a handheld metal detector used within three inches of the individual searched	
PS.S-11.2	Searches	Prohibit personnel from entering/exiting the facility with digital recording devices (e.g., USB thumb drives, digital cameras, cell phones) and include the search of these devices as part of the exit search procedure.	
PS-11.3	Searches	Enforce the use of transparent plastic bags and food containers for any food brought into production areas.	
PS-11.4	Searches	Implement a dress code policy that prohibits the use of oversized clothing (e.g., baggy pants, oversized hooded sweatshirts).	
PS-11.5	Searches	Use numbered tamper-evident stickers/holograms to identify authorized devices that can be taken in and out of the facility.	
PS-11.6	Searches	Implement a process to test the exit search procedure.	
PS-11.7	Searches	Perform a random vehicle search process when exiting the facility parking lot.	
PS-11.8	Searches	Segregate replication lines that process highly sensitive content and perform searches upon exiting segregated areas.	
PS-11.9	Searches	Implement additional controls to monitor security guards activity.	

No.	Security Topic	Best Practice	Verizon Implementation
PS-12.0	Inventory Tracking	Implement a content asset management system to provide detailed tracking of physical assets (i.e., received from client created at the facility).	Inventory tracking of content assets are the responsibility of the customer as content is typically ingested from customer origin directly. The customer and asset management portal also serves as a repository of all physical assets of the CDN, including owners, configurations, and metadata. Asset management procedures are reviewed by independent external auditors during audits for our SOC 2, PCI DSS, and ISO/IEC 27001:2013 compliance. Not applicable: Verizon does not handle any physical assets for content under MPAA security constraints. Content is instead ingested electronically and pre-encrypted with security features deemed appropriate by the customer. Output of content is controlled by the customer configurations for content distribution through the CDN. The objective of a CDN is to distribute customer media content over the internet. It is the customer's responsibility to apply the necessary content protections to media content before it is ingested into the CDN.
PS-12.1	Inventory Tracking	Barcode or assign unique tracking identifier(s) to client assets and created media (e.g., tapes, hard drives) upon receipt and store assets in the vault when not in use.	
PS-12.2	Inventory Tracking	Retain asset movement transaction logs for at least one year.	
PS-12.3	Inventory Tracking	Review logs from content asset management system at least weekly and investigate anomalies.	
PS-12.4	Inventory Tracking	Use studio film title aliases when applicable on physical assets and in asset tracking systems.	
PS-12.5	Inventory Tracking	Implement and review a daily aging report to identify highly sensitive assets that are checked out from the vault and not checked back in.	
PS-12.6	Inventory Tracking	Lock up and log assets that are delayed or returned if shipments could not be delivered on time.	

No.	Security Topic	Best Practice	Verizon Implementation
PS-13.0	Inventory Counts	Perform a quarterly inventory count of each client's asset(s), reconcile against asset management records, and immediately communicate variances to clients.	The customer and asset management portal serves as a repository of all assets to include owners, configurations, and metadata. It is the customer's responsibility to use the available security and monitoring features for tracking, asset control, log retention etc. Asset management procedures are reviewed by independent external auditors during audits for our SOC 2, PCI DSS, and ISO/IEC 27001:2013 compliance. Not applicable: Verizon does not handle any physical assets for content under MPAA security constraints. Content is instead ingested electronically and pre-encrypted with security features deemed appropriate by the customer. Output of content is controlled by the customer configurations for content distribution through the CDN. The objective of a CDN is to distribute customer media content over the internet. It is the customer's responsibility to apply the necessary content protections to media content before it is ingested into the CDN.
PS-13.1	Inventory Counts	Segregate duties between the vault staff and individuals who are responsible for performing inventory counts.	
PS-14.0	Blank Media/ Raw Stock Tracking	Tag (e.g., barcode, assign unique identifier) blank stock/raw stock per unit when received.	Customers are responsible for control and ownership of their data and media assets.
PS-14.1	Blank Media/ Raw Stock Tracking	Establish a process to track consumption of raw materials (e.g., polycarbonate) monthly.	
PS-14.2	Blank Media/ Raw Stock Tracking	Store blank media/raw stock in a secured location.	

No.	Security Topic	Best Practice	Verizon Implementation
PS-15.0	Client Assets	Restrict access to finished client assets to personnel responsible for tracking and managing assets.	Not applicable: Verizon does not handle any physical assets for content under MPAA security constraints. Content is instead ingested electronically and pre-encrypted with security features deemed appropriate by the customer. Output of content is controlled by the customer configurations for content distribution through the CDN. The objective of a CDN is to distribute customer media content over the internet. It is the customer's responsibility to apply the necessary content protections to media content before it is ingested into the CDN. Customers are responsible for control and ownership of their data and media assets.
PS-15.1	Client Assets	Store client assets in a restricted and secure area (e.g., vault, safe, or other secure storage location).	
PS-15.2	Client Assets	Require two company personnel with separate access cards to unlock highly sensitive areas (e.g., safe, high-security cage) after-hours.	
PS-15.3	Client Assets	Use a locked fireproof safe to store undelivered packages that are kept at the facility overnight.	
PS-15.4	Client Assets	Implement a dedicated, secure area (e.g., security cage, secure room) for the storage of undelivered screeners that is locked, access-controlled, and monitored with surveillance cameras and/or security guards.	
PS-16.0	Disposals	Require that rejected, damaged, and obsolete stock containing client assets are erased, degaussed, shredded, or physically destroyed before disposal.	Not applicable: Verizon does not handle any physical assets for content under MPAA security constraints. Content is instead ingested electronically and pre-encrypted with security features deemed appropriate by the customer. Output of content is controlled by the customer configurations for content distribution through the CDN. The objective of a CDN is to distribute customer media content over the internet. It is the customer's responsibility to apply the necessary content protections to media content before it is ingested into the CDN. Verizon leverages a Secure Packaging Delivery and Repurposing Procedure that includes a DoD solution to wipe all hard drives prior to disposal. This is managed between DC Operations and Security Operations. The Purge feature allows customers to remove the cached version of an asset from all edge servers and origin shield servers. A purge can be performed on a folder or an individual asset. Asset Management processes and procedures are reviewed by independent external auditors during audits for our PCI DSS and ISO/IEC 27001:2013 compliance.
PS-16.1	Disposals	Store elements targeted for recycling/destruction in a secure location/container to prevent the copying and reuse of assets prior to disposal.	
PS-16.2	Disposals	Maintain a log of asset disposal for at least 12 months.	
PS-16.3	Disposals	Destruction must be performed on site. On site destruction must be supervised and signed off by two company personnel. If a third-party destruction company is engaged, destruction must be supervised and signed off by two company personnel and certificates of destruction must be retained.	
PS-16.4	Disposals	Use automation to transfer rejected discs from replication machines directly into scrap bins (no machine operator handling).	

No.	Security Topic	Best Practice	Verizon Implementation
PS-17.0	Shipping	Require the facility to generate a valid work/shipping order to authorize client asset shipments out of the facility.	Not applicable: Verizon does not handle any physical assets for content under MPAA security constraints. Content is instead ingested electronically and pre-encrypted with security features deemed appropriate by the customer. Output of content is controlled by the customer configurations for content distribution through the CDN. The objective of a CDN is to distribute customer media content over the internet. It is the customer's responsibility to apply the necessary content protections to media content before it is ingested into the CDN. Customers retain control and ownership of their data and media assets. It is the responsibility of the Studio / Processing facility to manage security of media stock. Verizon leverages a Secure Packaging Delivery and Repurposing Procedure that requires the creation and approval of work orders to authorize shipments in and out of a data center. Shipping details are captured in a work order ticketing system and include: • Time of shipment • Sender name and signature • Recipient name • Address of destination • Tracking number from courier • Reference to the corresponding work order Asset Management processes and procedures are reviewed by independent external auditors during audits for our PCI DSS and ISO/IEC 27001:2013 compliance.
PS-17.1	Shipping	Track and log client asset shipping details; at a minimum, include the following: • Time of shipment • Sender name and signature • Recipient name • Address of destination • Tracking number from courier • Reference to the corresponding work order	
PS-17.2	Shipping	Secure client assets that are waiting to be picked up.	
PS-17.3	Shipping	Validate client assets leaving the facility against a valid work/ shipping order.	
PS-17.4	Shipping	Prohibit couriers and delivery personnel from entering content/ production areas of the facility.	
PS-17.5	Shipping	Document and retain a separate log for truck driver information.	
PS-17.6	Shipping	Observe and monitor the on-site packing and sealing of trailers prior to shipping.	
PS-17.7	Shipping	Record, monitor and review travel times, routes, and delivery times for shipments between facilities.	
PS-17.8	Shipping	Prohibit the transfer of film elements other than for client studio approved purposes.	
PS-17.9	Shipping	Ship prints for pre-theatrical screenings in segments (e.g., odd versus even reels).	

No.	Security Topic	Best Practice	Verizon Implementation
PS-18.0	Receiving	Inspect delivered client assets upon receipt and compare to shipping documents (e.g., packing slip, manifest log).	Not applicable: Verizon does not handle any physical assets for content under MPAA security constraints. Content is instead ingested electronically and pre-encrypted with security features deemed appropriate by the customer. Output of content is controlled by the customer configurations for content distribution through the CDN. The objective of a CDN is to distribute customer media content over the internet. It is the customer's responsibility to apply the necessary content protections to media content before it is ingested into the CDN.
PS-18.1	Receiving	Maintain a receiving log to be filled out by designated personnel upon receipt of deliveries.	
PS-18.2	Receiving	Perform the following actions immediately: • Tag (e.g., barcode, assign unique identifier) received assets • Input the asset into the asset management system • Move the asset to the restricted area (e.g., vault, safe)	
PS-18.3	Receiving	Implement a secure method for receiving overnight deliveries.	

No.	Security Topic	Best Practice	Verizon Implementation
PS-19.0	Labeling	Prohibit the use of title information, including AKAs ("aliases"), on the outside of packages unless instructed otherwise by client.	Not applicable: Verizon does not handle clients' physical asset inventory. Any content under MPAA security constraints is ingested electronically and pre-encrypted with security features deemed appropriate by the customer. Packaging of any physical finished media assets are the responsibility of the customer. Asset Management processes and procedures are reviewed by independent external auditors during audits for our PCI DSS and ISO/IEC 27001:2013 compliance.
PS-20.0	Packaging	Ship all client assets in closed/ sealed containers, and use locked containers depending on asset value, or if instructed by the client.	Not applicable: Verizon does not handle any physical assets for content under MPAA security constraints. Content is instead ingested electronically and pre-encrypted with security features deemed appropriate by the customer. Output of content is controlled by the customer configurations for content distribution through the CDN. The objective of a CDN is to distribute customer media content over the internet. It is the customer's responsibility to apply the necessary content protections to media content before it is ingested into the CDN. Packaging of any physical finished media assets is the responsibility of the customer.
PS-20.1	Packaging	Implement at least one of the following controls: • Tamper-evident tape • Tamper-evident packaging • Tamper-evident seals (e.g., in the form of holograms) • Secure containers (e.g., Pelican case with a combination lock)	
PS-20.2	Packaging	Apply shrink wrapping to all shipments, and inspect packaging before final shipment to ensure that it is adequately wrapped.	
PS-21.0	Transport Vehicles	Lock automobiles and trucks at all times, and do not place packages in visible auto/truck areas	Not applicable: Verizon does not handle any physical assets for content under MPAA security constraints. Content is instead ingested electronically and pre-encrypted with security features deemed appropriate by the customer. Output of content is controlled by the customer configurations for content distribution through the CDN. The objective of a CDN is to distribute customer media content over the internet. It is the customer's responsibility to apply the necessary content protections to media content before it is ingested into the CDN. Transport of any physical finished media assets are the responsibility of the customer.
PS-21.1	Transport Vehicles	Include the following security features in transportation vehicles (e.g., trailers): • Segregation from driver cabin • Ability to lock and seal cargo area doors • GPS for high-security shipments	
PS-21.2	Transport Vehicles	Apply numbered seals on cargo doors for shipments of highly sensitive titles.	
PS-21.3		Require security escorts to be used when delivering highly sensitive content to high-risk areas.	

No.	Security Topic	Best Practice	Verizon Implementation
DS-1.0	Firewall/WAN	Separate external network(s)/ WAN(s) from the internal network(s) by using inspection firewall(s) with Access Control Lists that prevent unauthorized access to any internal network and with the ability to keep up with upload and download traffic.	Network Operations and System Operations manages the port, protocol, application and services installed on all devices. This is documented within the hardening procedures. Security Operations audits the configurations to ensure they are configured per the procedure. Network ACL audits are performed quarterly. On completion of initial firewall configurations, the VP of Network Engineering convenes a Firewall Review Board comprised of appropriately trained and vetted resources and the VP of Network Engineering. The Network Review Board audits the submitted configuration. Once accepted, the firewall configuration is saved to a file repository and is further deemed the Base Installation. The necessity of performing firewall software updates is assessed by the Network Engineering team using vendor-provided update information as well as more generalized security guidelines. Verizon has implemented an automated system of vulnerability management for all IT systems, devices and appliances, regardless of operating system or platform. This consists of clearly assigned specific responsibilities for the System Administrator(s) or other authorized personnel. They direct systems administrators to subscribe to industry and vendor alerts in order to receive timely information on new vulnerabilities. Internal vulnerability scans occur monthly or after any major changes to the environment. External vulnerability scans occur at least daily. External quarterly scans pertaining to PCI DSS requirements are performed by a PCI SSC Approved Scanning Vendor (ASV). Internal and external penetration testing occurs at least annually and after any major infrastructure change. Testing includes both network and application-level tests. Reports and evidence are centrally maintained. It is the customer's responsibility to encrypt content by using SSL/TLS and SSL Certificates. Network Time Protocol (NTP) is implemented throughout the CDN.
DS-1.1	Firewall/WAN	Implement a process to review firewall Access Control Lists (ACLs) to confirm configuration settings are appropriate and required by the business every 6 months.	
DS-1.2	Firewall/WAN	Deny all protocols by default and enable only specific permitted secure protocols to access the WAN and firewall.	
DS-1.3	Firewall/WAN	Place externally accessible servers (e.g., web servers) within the DMZ.	
DS-1.4	Firewall/WAN Perimeter Security	Implement a process to patch network infrastructure devices (e.g., firewalls, routers, switches, etc.), SAN/NAS (Storage Area Networks and Network Attached Storage), and servers.	
DS-1.5	Firewall/WAN	Harden network infrastructure devices, SAN/NAS, and servers based on security configuration standards. Disable SNMP (Simple Network Management Protocol) if it is not in use or use only SNMPv3 or higher and select SNMP community strings that are strong passwords.	
DS-1.6	Firewall/WAN	Do not allow remote management of the firewall from any external interface(s).	

No.	Security Topic	Best Practice	Verizon Implementation
DS-1.7	Firewall/WAN	Secure backups of network infrastructure/SAN/NAS devices and servers to a centrally secured server on the internal network.	Network Operations and System Operations manages the port, protocol, application and services installed on all devices. This is documented within the hardening procedures. Security Operations audits the configurations to ensure they are configured per the procedure. Network ACL audits are performed quarterly. On completion of initial firewall configurations, the VP of Network Engineering convenes a Firewall Review Board comprised of appropriately trained and vetted resources and the VP of Network Engineering. The Network Review Board audits the submitted configuration. Once accepted, the firewall configuration is saved to a file repository and is further deemed the Base Installation. The necessity of performing firewall software updates is assessed by the Network Engineering team using vendor-provided update information as well as more generalized security guidelines. Verizon has implemented an automated system of vulnerability management for all IT systems, devices and appliances, regardless of operating system or platform. This consists of clearly assigned specific responsibilities for the System Administrator(s) or other authorized personnel. They direct systems administrators to subscribe to industry and vendor alerts in order to receive timely information on new vulnerabilities. Internal vulnerability scans occur monthly or after any major changes to the environment. External vulnerability scans occur at least daily. External quarterly scans pertaining to PCI DSS requirements are performed by a PCI SSC Approved Scanning Vendor (ASV). Internal and external penetration testing occurs at least annually and after any major infrastructure change. Testing includes both network and application-level tests. Reports and evidence are centrally maintained. It is the customer's responsibility to encrypt content by using SSL/TLS and SSL Certificates. Network Time Protocol (NTP) is implemented throughout the CDN.
DS-1.8	Firewall/WAN	Perform quarterly vulnerability scans of all external IP ranges and hosts at least and remediate issues.	
DS-1.9	Firewall/WAN	Perform annual penetration testing of all external IP ranges and hosts at least and remediate issues.	
DS-1.10	Firewall/WAN	Secure any point to point connections by using dedicated, private connections and by using encryption.	
DS-1.11	Firewall/WAN	Implement a synchronized time service protocol (e.g., Network Time Protocol) to ensure all systems have a common time reference.	
DS-1.12	Firewall/WAN	Establish, document and implement baseline security requirements for WAN network infrastructure devices and services.	

No.	Security Topic	Best Practice	Verizon Implementation
DS-2.0	Internet	Prohibit production network and all systems that process or store digital content from directly accessing the internet, including email. If a business case requires internet access from the production network or from systems that process or store digital content, only approved methods are allowed via use of a remote hosted application / desktop session.	Not applicable: The objective of a CDN is to distribute customer media content over the internet. It is the customer's responsibility to apply the necessary content protections to media content before it is ingested into the CDN. Packaging of any physical finished media assets is the responsibility of the customer.
DS-2.1	Internet	Implement email filtering software or appliances that block the following from non-production networks: • Potential phishing emails • Prohibited file attachments (e.g., Visual Basic scripts, executables, etc.) • File size restrictions limited to 10 MB • Known domains that are sources of malware or viruses	
DS-2.2	Internet	Implement web filtering software or appliances that restrict access to websites known for peer-to-peer file trading, viruses, hacking or other malicious sites.	

No.	Security Topic	Best Practice	Verizon Implementation
DS-3.0	LAN/Internal Network	Isolate the content/production network from non-production networks (e.g., office network, DMZ, the internet etc.) by means of physical or logical network segmentation.	The network has been designed to segment production, development and staging environments with VLANs and ACLs. The DLA testing environment is a logically and physically segregated non-production environment. Verizon restricts access through logical authentication and authorization mechanisms, to include: • Two-factor authentication • Virtual Private Networks • Jumpbox segmentation for access control • Active Directory authentication Verizon Switch and Router Port Policy details that network device ports not actively forwarding traffic are administratively shut down. Further, new switches that are shipped and scheduled for deployment have all non-uplink/stack ports disabled before shipping. An intrusion detection and/or intrusion prevention system operates on each network segment with sensitive information, and is configured to alert security personnel of potential compromises. File Integrity monitoring software is configured to prevent unauthorized modification of system files, log files, and critical application files. Vulnerability scans are conductd on a quarterly basis in accordance with industry best practices. Network security policies and procedures are reviewed by independent external auditors during audits for our PCI DSS and ISO/IEC 27001:2013 compliance.
DS-3.1	LAN/Internal Network	Restrict access to the content/production systems to authorized personnel.	
DS-3.2	LAN/Internal Network	Restrict remote access to the content/production network to only approved personnel who require access to perform their job responsibilities.	
DS-3.3	LAN/Internal Network	Use switches/layer 3 devices to manage the network traffic, and disable all unused switch ports on the content/production network to prevent packet sniffing by unauthorized devices.	
DS-3.4	LAN/Internal Network	Restrict the use of non-switched devices such as hubs and repeaters on the content/ production network.	
DS-3.5	LAN/Internal Network	Prohibit dual-homed networking (physical networked bridging) on computer systems within the content/production network.	
DS-3.6	LAN/Internal Network	Implement a network-based intrusion detection/prevention system (IDS/IPS) on the content/ production network.	
DS-3.7	LAN/Internal Network	Disable SNMP (Simple Network Management Protocol) if it is not in use or uses only SNMPv3 or higher and select SNMP community strings that are strong passwords.	
DS-3.8	LAN/Internal Network	Harden systems prior to placing them in the LAN/Internal Network.	
DS-3.9	LAN/Internal Network	Conduct internal network vulnerability scans and remediate any issues, at least annually.	
DS-3.10	LAN/Internal Network	Secure backups of local area network SAN/NAS, devices, servers and workstations to a centrally secured server on the internal network.	

No.	Security Topic	Best Practice	Verizon Implementation
DS-4.0	Wireless	Prohibit wireless networking and the use of wireless devices on the content/production network.	Wireless networking is prohibited on the content network. Testing occurs through quarterly walkthroughs of production facilities with a laptop or automated wireless intrusion detection system (IDS) to identify wireless rogue access points. Corporate (non-production) WIFI uses Active Directory for authentication and WPA2 enterprise – AES encryption. A separate guest network is available and separate from the company's other wireless networks. Network security policies and procedures are reviewed by independent external auditors during audits for our PCI DSS and ISO/IEC 27001:2013 compliance.
DS-4.1	Wireless	Configure non-production wireless networks (e.g., administrative and guest) with the following security controls: • Disable WEP/WPA • Only Enable AES128 encryption (WPA2), or higher • Segregate "guest" networks from the company's other networks • Change default administrator logon credentials • Change default network name (SSID)	
DS-4.2	Wireless	Implement a process to scan for rogue wireless access points and remediate any validated issues.	
DS-5.0	I/O Device Security	Designate specific systems to be used for content input/output (I/O).	Not applicable: Verizon does not handle any physical assets for content under MPAA security constraints. Content is instead ingested electronically and pre-encrypted with security features deemed appropriate by the customer. Output of content is controlled by the customer configurations for content distribution through the CDN. The objective of a CDN is to distribute customer media content over the internet. It is the customer's responsibility to apply the necessary content protections to media content before it is ingested into the CDN. In order to prevent unauthorized users and websites from linking (a.k.a. hot linking) to content and leveraging customer bandwidth or other types of misuse, Verizon provides a Token-Based Authentication feature. Using this technology, a customer can create a private key and use that key to pass certain dynamically created, encrypted values via the URL string to Verizon. Verizon servers will then use these values to grant or deny access to the content. Dedicated SSL certificates can also be provisioned on a per tenant basis.
DS-5.1	I/O Device Security	Block input/output (I/O), mass storage, external storage, and mobile storage devices (e.g., USB, FireWire, Thunderbolt, SATA, SCSI, etc.) and optical media burners (e.g., DVD, Blu-Ray, CD, etc.) on all systems that handle or store content, with the exception of systems used for content I/O.	

No.	Security Topic	Best Practice	Verizon Implementation
DS-6.0	System Security	Install anti-virus and anti-malware software on all workstations, servers, and on any device that connects to SAN/NAS systems.	Verizon Security and availability policies are available that promulgate policy for: • Hardening standards • Base install standards • Server configurations for multiple platforms • Patching procedures. Desktop computers are loaded with anti-virus software. Routine scanning and threat mitigation contribute to a holistic security environment across the schema. Corporate workstations and devices are equipped with commercial-grade antivirus software. In the event of a threat detection, Incident Response and Disaster Recovery procedures are published and understood by employees. All end devices connecting to the Verizon corporate network are required to have the standard and supported antivirus software installed and scheduled to run at regular intervals. In addition, the antivirus software and the virus signature files must be kept automatically up-to-date. The antivirus software must be configured to scan in real time. Users are responsible for ensuring antivirus software is run at regular intervals, and computers are verified as virus-free. Verizon ensures software is capable of detecting, removing, and protecting against viruses and other forms of malicious software, including spyware and adware, and its capability of generating audit logs. Virus-infected computers must be removed from the network until they are verified as virus-free. Patch management is used in conjunction with the normal vulnerability testing efforts. All authorized personnel are trained in system administration to include patch management techniques. An organizational hardware and software inventory is maintained, and an electronic database of information on patches required and deployed on the systems or applications for the purposes of proper internal controls and reporting to external entities within constrained timeframes. Patches are tested on non-production systems prior to installation on any production systems. A standardized build in regard to hardware configuration also enables a more fluid and correct architecture for patches. Security updates are also streamlined under this model. System security policies and procedures are reviewed by independent external auditors during audits for our PCI DSS and ISO/IEC 27001:2013 compliance. Token-Based Authentication provides security for assets accessed through the Verizon Digital Media Services CDN. Only authorized users that provide the appropriate token for the requested asset will be able to access a customer's content.
DS-6.1	System Security	Update all anti-virus and anti-malware definitions daily, or more frequently.	
DS-6.2	System Security	Scan all content for viruses and malware prior to ingest onto the content/production network.	
DS-6.3	System Security	Perform scans as follows: • Enable regular full system virus and malware scanning on all workstations • Enable full system virus and malware scans for servers and for systems connecting to a SAN/NAS	
DS-6.4	System Security	Implement a process to regularly update systems (e.g., file transfer systems, operating systems, databases, applications, network devices) with patches/updates that remediate security vulnerabilities.	
DS-6.5	System Security	Prohibit users from being Administrators on their own workstations, unless required for software (e.g., ProTools, Clipster and authoring software such as Blu-Print, Scenarist and Toshiba). Documentation from the software provider must explicitly state that administrative rights are required.	
DS-6.6	System Security	Use cable locks on portable computing devices that handle content (e.g., laptops, tablets, towers) when they are left unattended.	
DS-6.7	System Security	Implement additional security controls for laptops and portable computing storage devices that contain content or sensitive information relating to client projects. Encrypt all laptops. Use hardware-encrypted portable computing storage devices. Install remote-kill software on all laptops/mobile devices that handle content to allow remote wiping of hard drives and other storage devices.	

No.	Security Topic	Best Practice	Verizon Implementation
DS-6.8	System Security	Restrict software installation privileges to IT management.	Verizon Security and availability policies are available that promulgate policy for: • Hardening standards • Base install standards • Server configurations for multiple platforms • Patching procedures. Desktop computers are loaded with anti-virus software. Routine scanning and threat mitigation contribute to a holistic security environment across the schema. Corporate workstations and devices are equipped with commercial-grade antivirus software. In the event of a threat detection, Incident Response and Disaster Recovery procedures are published and understood by employees. All end devices connecting to the Verizon corporate network are required to have the standard and supported antivirus software installed and scheduled to run at regular intervals. In addition, the antivirus software and the virus signature files must be kept automatically up-to-date. The antivirus software must be configured to scan in real time. Users are responsible for ensuring antivirus software is run at regular intervals, and computers are verified as virus-free. Verizon ensures software is capable of detecting, removing, and protecting against viruses and other forms of malicious software, including spyware and adware, and its capability of generating audit logs. Virus-infected computers must be removed from the network until they are verified as virus-free. Patch management is used in conjunction with the normal vulnerability testing efforts. All authorized personnel are trained in system administration to include patch management techniques. An organizational hardware and software inventory is maintained, and an electronic database of information on patches required and deployed on the systems or applications for the purposes of proper internal controls and reporting to external entities within constrained timeframes. Patches are tested on non-production systems prior to installation on any production systems. A standardized build in regard to hardware configuration also enables a more fluid and correct architecture for patches. Security updates are also streamlined under this model. System security policies and procedures are reviewed by independent external auditors during audits for our PCI DSS and ISO/IEC 27001:2013 compliance. Token-based authentication provides security for assets accessed through the Verizon Digital Media Services CDN. Only authorized users that provide the appropriate token for the requested asset will be able to access a customer's content.
DS-6.9	System Security	Implement security baselines and standards to configure systems (e.g., laptops, workstations, servers, SAN/NAS) that are set up internally.	
DS-6.10	System Security	Unnecessary services and applications should be uninstalled from content transfer servers.	
DS-6.11	System Security	Maintain an inventory of systems and system components.	
DS-6.12	System Security	Document the network topology and update the diagram annually or when significant changes are made to the infrastructure.	

No.	Security Topic	Best Practice	Verizon Implementation
DS-7.0	Account Management	Establish and implement an account management process for administrator, user, and service accounts for all information systems and applications that handle content.	Verizon Digital Media Services Security and Availability policies address the following: • Identifying and documenting security requirements of authorized users. • Credentialing employees per written policy. • Identifying 'need to know' access to systems. • Tiered and collaborative account creation process that involves Human Resources, IT Department, Information Security team, and other elements to ensure cohesive and proper account creations and role assignment. • A termination checklist that systematically removes former employee permissions and access. • A vetting process also collaborated between management and information systems owners that elevates or otherwise adjusts user permissions as work responsibilities require. Access Management processes and procedures are reviewed by independent external auditors during audits for our PCI DSS and ISO/IEC 27001:2013 compliance.
DS-7.1	Account Management	Maintain traceable evidence of the account management activities (e.g., approval emails, change request forms).	
DS-7.2	Account Management	Assign unique credentials on a need-to-know basis using the principles of least privilege.	
DS-7.3	Account Management	Rename the default administrator accounts and other default accounts and limit the use of these accounts to special situations that require these credentials (e.g., operating system updates, patch installations, software updates).	
DS-7.4	Account Management	Segregate duties to ensure that individuals responsible for assigning access to information systems are not themselves end users of those systems (i.e., personnel should not be able to assign access to themselves).	
DS-7.5	Account Management	Monitor and audit administrator and service account activities.	
DS-7.6	Account Management	Implement a process to review user access for all information systems that handle content and remove any user accounts that no longer require access quarterly.	
DS-7.7	Account Management	Restrict user access to content on a per-project basis.	
DS-7.8	Account Management	Disable or remove local accounts on systems that handle content where technically feasible.	

No.	Security Topic	Best Practice	Verizon Implementation
DS-8.0	Authentication	Enforce the use of unique usernames and passwords to access information systems.	Verizon restricts access through logical authentication and authorization mechanisms, to include: • Two-factor authentication • Virtual Private Networks • Jumpbox segmentation for access control • Active Directory authentication Password policies are enforced via GPO reviewed by independent external auditors during audits for our PCI DSS and ISO/IEC 27001:2013 compliance.
DS-8.1	Authentication	Enforce a strong password policy for gaining access to information systems.	
DS-8.2	Authentication	Implement two-factor authentication (e.g., username/ password and hard token) for remote access (e.g., VPN) to the networks.	
DS-8.3	Authentication	Implement password-protected screensavers or screen-lock software for servers and workstations.	
DS-8.4	Authentication	Consider implementing additional authentication mechanisms to provide a layered authentication strategy for WAN and LAN/ Internal Network access.	

No.	Security Topic	Best Practice	Verizon Implementation
DS-9.0	Logging and Monitoring	Enable logging of internal and external content movement and transfers and include the following information at a minimum: • Username • Timestamp • File name • Source IP address • Destination IP address Event (e.g., download, view)	Verizon ensures software is capable of detecting, removing, and protecting against viruses and other forms of malicious software, including spyware and adware, and its capability of generating audit logs. Virus-infected computers must be removed from the network until they are verified as virus-free. An intrusion detection and/or intrusion prevention system operates on each network segment with credit card data or other sensitive information, and is configured to alert security personnel of potential compromises. File Integrity monitoring software is configured to prevent unauthorized modification of system files, log files, and critical application files. Human control is exercised on a 24 hour-a-day basis and physical monitors display network analytics and measurements for all services, in addition to the active alerts that are triggered by significant events. Additionally, specialized programs have been developed within Verizon and deployed across the operating aspects of the company's functional areas. Logs are generated by all production servers, including key generation and management servers centrally stored on syslog/log management servers. Security alerts are automatically generated and reviewed daily. Access to syslog servers is restricted to security personnel. Logging and monitoring processes are reviewed by independent external auditors during audits for our PCI DSS and ISO/IEC 27001:2013 compliance.
DS-9.1	Logging and Monitoring	Implement a server to manage the logs in a central repository (e.g., syslog/log management server, Security Information and Event Management (SIEM) tool).	
DS-9.2	Logging and Monitoring	Configure logging systems to send automatic notifications when security events are detected in order to facilitate active response to incidents.	
DS-9.3	Logging and Monitoring	Investigate any unusual activity reported by the logging and reporting systems.	
DS-9.4	Logging and Monitoring	Implement logging mechanisms on all systems used for the following: • Key generation • Key management • Vendor certificate management	
DS-9.4	Logging and Monitoring	Review all logs weekly, and review all critical and high daily.	
DS-9.5	Logging and Monitoring	Enable logging of internal and external content movement and transfers and include the following information at a minimum: • Username • Timestamp • File name • Source IP address • Destination IP address Event (e.g., download, view)	
DS-9.6	Logging and Monitoring	Retain logs for at least one year.	
DS-9.7	Restrict log access to appropriate personnel	Restrict log access to appropriate personnel.	

No.	Security Topic	Best Practice	Verizon Implementation
DS-10.0	Mobile Security	Develop a BYOD (Bring Your Own Device) policy for mobile devices accessing or storing content.	Verizon Digital Media Services has implemented a BYOD policy that implements the following: • Restricts mobile access to email and calendars only. Mobile devices devices are not allowed to access the production network. • Standard security controls such as encryption, passwords, anti-virus and automatic locking of the device following a period of inactivity. • Remote location/remote wipe is used to handle lost or stolen devices.
DS-10.1	Mobile Security	Develop a BYOD (Bring Your Own Device) policy for mobile devices accessing or storing content.	
DS-10.2	Mobile Security	Maintain an inventory of all mobile devices that access or store content.	
DS-10.3	Mobile Security	Require encryption either for the entire device or for areas of the device where content will be handled or stored.	
DS-10.4	Mobile Security	Prevent the circumvention of security controls.	
DS-10.5	Mobile Security	Implement a system to perform a remote wipe of a mobile device, should it be lost/stolen/compromised or otherwise necessary.	
DS-10.6	Mobile Security	Implement automatic locking of the device after 10 minutes of non-use.	
DS-10.7	Mobile Security	Manage all mobile device operating system patches and application updates.	
DS-10.8	Mobile Security	Enforce password policies.	
DS-10.9	Mobile Security	Implement a system to perform backup and restoration of mobile devices.	

No.	Security Topic	Best Practice	Verizon Implementation
DS-11.0	Security Techniques	Ensure that security techniques (e.g., spoiling, invisible/visible watermarking) are available for use and are applied when instructed.	Not applicable: Verizon Digital Media Services does not handle any physical assets for content under MPAA security constraints. Content is instead ingested electronically and pre-encrypted with security features deemed appropriate by the customer. Output of content is controlled by the customer configurations for content distribution through the CDN. The objective of a CDN is to distribute customer media content over the internet. It is the customer's responsibility to apply the necessary content protections to media content before it is ingested into the CDN. Verizon Digital Media Services has a number of encryption management solutions in place to protect client information and the streaming of said information. Cryptographic processes are reviewed by independent external auditors during audits for our PCI DSS and ISO/IEC 27001:2013 compliance.
DS-11.1	Security Techniques	Encrypt content on hard drives or encrypt entire hard drives using a minimum of AES 128-bit, or higher, encryption by either: • File-based encryption: (i.e., encrypting the content itself) • Drive-based encryption: (i.e., encrypting the hard drive)	
DS-11.2	Security Techniques	Send decryption keys or passwords using an out-of-band communication protocol (i.e., not on the same storage media as the content itself).	
DS-11.3	Security Techniques	Implement and document key management policies and procedures: • Use of encryption protocols for the protection of sensitive content or data, regardless of its location (e.g., servers, databases, workstations, laptops, mobile devices, data in transit, email) • Approval and revocation of trusted devices • Generation, renewal, and revocation of content keys • Internal and external distribution of content keys • Bind encryption keys to identifiable owners • Segregate duties to separate key management from key usage • Key storage procedures • Key backup procedures	
DS-11.4	Security Techniques	Encrypt content at rest and in motion, including across virtual server instances, using a minimum of AES 128-bit, or higher, encryption.	

No.	Security Topic	Best Practice	Verizon Implementation
DS-11.5	Security Techniques	Store secret and private keys (not public keys) used to encrypt data/content in one or more of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (e.g., Host Security Module (HSM) or a Pin Transaction Security (PTS) point-of-interaction device) • Has at least two full-length key components or key shares, in accordance with a security industry accepted method	Not applicable: Verizon Digital Media Services does not handle any physical assets for content under MPAA security constraints. Content is instead ingested electronically and pre-encrypted with security features deemed appropriate by the customer. Output of content is controlled by the customer configurations for content distribution through the CDN. The objective of a CDN is to distribute customer media content over the internet. It is the customer's responsibility to apply the necessary content protections to media content before it is ingested into the CDN. Verizon Digital Media Services has a number of encryption management solutions in place to protect client information and the streaming of said information. Cryptographic processes are reviewed by independent external auditors during audits for our PCI DSS and ISO/IEC 27001:2013 compliance.
DS-11.6	Security Techniques	Confirm that devices on the Trusted Devices List (TDL) are appropriate based on rights owners' approval.	
DS-11.7	Security Techniques	Confirm the validity of content keys and ensure that expiration dates conform to client instructions.	
DS-12.0	Content Tracking	Implement a digital content management system to provide detailed tracking of digital content.	Verizon Digital Media Services provides a rich suite of features to protect our customers, their end-users, and publishing relationships through the use of the customer portal. Advanced reporting is an optional feature available to assist customers in tracking their digital content. HTTP/S transaction logs are retained for at least one year and can be reviewed to investigate anomolies.
DS-12.1	Content Tracking	Retain digital content movement transaction logs for one year.	
DS-12.2	Content Tracking	Review logs from digital content management system periodically and investigate anomalies.	
DS-12.3	Content Tracking	Use client AKAs ("aliases") when applicable in digital asset tracking systems.	
DS-13.0	Transfer Systems	Use only client-approved transfer systems that utilize access controls, a minimum of AES 128-bit, or higher, encryption for content at rest and for content in motion and use strong authentication for content transfer sessions.	Secure file transfer and encryption services are available for customer use.
DS-13.1	Transfer Systems	Implement an exception process, where prior client approval must be obtained in writing, to address situations where encrypted transfer tools are not used.	

No.	Security Topic	Best Practice	Verizon Implementation
DS-14.0	Transfer Device Methodology	Implement and use dedicated systems for content transfers.	Not applicable: Verizon Digital Media Services does not handle any physical assets for content under MPAA security constraints. Content is instead ingested electronically and pre-encrypted with security features deemed appropriate by the customer. Output of content is controlled by the customer configurations for content distribution through the CDN. The objective of a CDN is to distribute customer media content over the internet. It is the customer's responsibility to apply the necessary content protections to media content before it is ingested into the CDN. Verizon Digital Media Services has a number of encryptions.
DS-14.1	Transfer Device Methodology	Separate content transfer systems from administrative and production networks.	
DS-14.2	Transfer Device Methodology	Place content transfer systems in a Demilitarized Zone (DMZ) and not in the content/production network.	
DS-14.3	Transfer Device Methodology	Remove content from content transfer devices/systems immediately after successful transmission/receipt.	
DS-14.4	Transfer Device Methodology	Send automatic notifications to the production coordinator(s) upon outbound content transmission.	Not applicable: Verizon Digital Media Services does not handle any physical assets for content under MPAA security constraints. Content is instead ingested electronically and pre-encrypted with security features deemed appropriate by the customer. Output of content is controlled by the customer configurations for content distribution through the CDN. The objective of a CDN is to distribute customer media content over the internet. It is the customer's responsibility to apply the necessary content protections to media content before it is ingested into the CDN.

No.	Security Topic	Best Practice	Verizon Implementation
DS-15.0	Client Portal	Restrict access to web portals which are used for transferring content, streaming content and key distribution to authorized users.	Verizon Digital Media Services designed its services with the assumption that certain controls would be implemented by user entities. These controls should be in operation at user entities to complement Verizon Digital Media Services controls. The user entity controls subsequently presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. User entities of Verizon Digital Media Services platform-as-a-service system should maintain controls to provide reasonable assurance that: • User access to Verizon Digital Media Services platform (portals, APIs) is restricted to authorized employees and requires that user names and passwords are kept confidential. • User access to Verizon Digital Media Services platform is periodically reviewed. • Password and user access modification requests are submitted and responded to in a timely manner. Access to the Portal is only available from a secure internet browser using the SSL (HTTPS) protocol and is controlled by a user name and password. Each user has control over their own password and has the ability to change their password when they wish. In addition, two-factor authentication can be enabled for the Portal account, requiring the user to enter a system-generated token, as well as their password, at login time. The token will be delivered to the user via their pre-defined method (e.g., via SMS). User utility PORTAL authentication is achieved with multiple authentication vectors: two-factor authentication and user name and password. Internal and external penetration testing occurs at least annually and after any major infrastructure change. Testing includes both network and application-level tests. Reports and evidence are centrally maintained.
DS-15.1	Client Portal	Assign unique credentials (e.g., username and password) to portal users and distribute credentials to clients securely.	
DS-15.2	Client Portal	Ensure users only have access to their own digital assets (i.e., client A must not have access to client B's content).	
DS-15.3	Client Portal	Place the web portal on a dedicated server in the DMZ and limit access to/from specific IPs and protocols.	
DS-15.4	Client Portal	Prohibit the use of third-party production software/systems/ services that are hosted on an internet web server unless approved by client in advance.	
DS-15.5	Client Portal	Use HTTPS and enforce use of a strong cipher suite (e.g., TLS v1) for the internal/external web portal.	
DS-15.6	Client Portal	Do not use persistent cookies or cookies that store credentials in plaintext.	
DS-15.7	Client Portal	Set access to content on internal or external portals to expire automatically at predefined intervals, where configurable.	
DS-15.8	Client Portal	Test for web application vulnerabilities quarterly and remediate any validated issues.	
DS-15.9	Client Portal	Perform annual penetration testing of web applications and remediate any validated issues.	
DS-15.10	Client Portal	Allow only authorized personnel to request the establishment of a connection with the telecom service provider.	
DS-15.11	Client Portal	Prohibit transmission of content using email (including webmail).	
DS-15.12	Client Portal	Review access to the client web portal at least quarterly.	

verizon

digital media services

Verizon Digital Media Services' next-generation platform brings together world-class technologies to prepare, deliver, display and enable the monetization of digital content so viewers can watch and enjoy on their terms. Built on one of the world's largest networks, Verizon Digital Media Services empowers content providers to deliver great viewer experiences for any content on every screen.

For more information on Verizon Digital Media Services, please visit **VerizonDigitalMedia.com**.