MPA Content Security Best Practices

Google Cloud Mapping

This document is designed to help organizations in the entertainment industry consider the Motion Pictures Association of America Security Best Practices Guidelines version 4.10, dated February 8, 2022 ("MPA guidance") in the context of Google Cloud .

We focus on the following requirements in Section V of the MPA Guidance on Best Practices Common Guidelines. For each paragraph of these Sections, we provide commentary to help you understand how you can address the MPA Guidance using the Google Cloud services.

#	Reference	Google Cloud Commentary
	I. Executive Security Awareness/Oversight	
MS-1.0	Establish an information security management system that implements a control framework for information security which is approved by the business owner(s) / senior management. Implementation Guidance: ● Reference established information and content security frameworks e.g. MPA Best Practices, ISO27001's, NIST 800-53, SANS, CoBIT, etc. ● Establish an independent team for information security. ● Persons responsible for information security should not be working on content.	Google maintains a robust and up-to-date Information Security Management System that is audited at least yearly and signed off by business leadership. As part of the ISO/IEC 27001 certified ISMS, roles and responsibilities are documented and authorized by leadership. Google performs risk assessments as required to support its ISMS. Google takes into account regulatory, legal, statutory or location restrictions of data, including data retention, classification and protection, in its risk assessments. Google has demonstrated adherence to this control by way of ISO/IEC 27001, ISO/IEC 27018 certification, as well as the annual external third party audits conducted for SOC 2/3 compliance. Google provides customers (under NDA) a copy of the SOC 2/3 report that demonstrates compliance with these controls. Information Security policies and procedures are communicated to all internal employees that must undergo and attest to yearly training.
MS-1.1	Review content / information security management policies and processes at least annually. Policies must be approved by senior management. Implementation Guidance: Consider adjustments to policies and procedures from the following changes: ● Organization's business, services offered, etc. ● Technology infrastructure ● Client requirements ● Regulations or laws ● Risk landscape	Google executive management reviews and approves all information security policies and sets applicable commitment and direction to achieve the agreed upon Information Security goals. Google reviews its security policies at least annually. Google's cross functional security policy team meets periodically throughout the year to address emerging issues and risks and issue new or amend existing policies or guidelines, as needed. See Row MS-1.3 Google continuously surveys its compliance landscape and adjusts its policies and practices as needed. It is the customer's responsibility to configure the services, per Google best practices, to be in compliance with any requirements relevant to their operations or jurisdictions. Google notifies tenants of material changes to our privacy policy. Our security policies are internal facing and we don't notify customers of changes.
MS-1.2	Train and engage executive management/owner(s) on the business' responsibilities to protect content at least annually. Implementation Guidance: ● Trainings and attendees should be documented in training logs	At Google, managers are responsible for ensuring their direct reports complete the required training and affidavits.Sanctions are put in place for Googlers who do not complete required training within the required time period. Annual security training is required for all Google Employees. Additional security training exists on the employee learning platform as well as periodic workshops. Google maintains a robust vendor management program. Vendors who work with Google are contractually required to comply with all relevant information security and privacy policies.
MS-1.3	Create an information security management group to establish and review information security management policies.	Google has a well defined information security organization with well-defined roles and responsibilities.

	Implementation Guidance: • Members of the information security management group should also attend security awareness training (see MS-1.2).	Google has a dedicated security team that is responsible for educating Google employees and contractors on security. Google has security policies that have been approved by management and published on the intranet which is accessible to all employees and contractors. Customers can review the Google Security Whitepaper to better understand Google's security strategy. Google undergoes several independent third party audits to test for data safety, privacy, and security, as noted below: • SOC 1 / 2 / 3 (Formerly SSAE16 or SAS 70) • ISO/IEC 27001 • ISO/IEC 27017/27018 • PCI-DSS • HIPAA Google publishes and makes available its ISO/IEC 27001, 27017, 27018 and SOC3 reports online. Detailed information of some confidential reports can be obtained under NDA.
	II. Risk Management	
MS-2.0	Develop a formal, documented security risk assessment process focused on content workflows and sensitive assets in order to identify and prioritize risks of content theft and leakage that are relevant to the facility. Implementation Guidance: • Define a clear scope for the security risk assessment and modify as necessary • Incorporate a systematic approach that uses likelihood of risk occurrence, impact to business objectives/content protection and asset classification for assigning priority • Ensure WFH/Remote access content workflow risks are also documented and addressed • Risks identified should tie into the business continuity and disaster recovery plan • Refer to MS-8.0 for best practices regarding documented workflows	Google performs risk assessments as required by ISO/IEC 27001. The risk assessment uses both qualitative and quantitative methods to determine likelihood and impact of events. Google reviews its security policies at least annually. Google's cross functional security policy team meets periodically throughout the year to address emerging issues and risk and issue new or amend existing policies or guidelines, as needed.
MS-2.1	Conduct an internal security risk assessment annually and upon key workflow changes—based on, at a minimum, the MPA Best Practice Common Guidelines and the applicable Supplemental Guidelines—and document and act upon identified risks. Implementation Guidance: • Conduct meetings with management and key stakeholders at least quarterly to identify and document content theft and leakage risks • Conduct external and internal network vulnerability scans and external penetration testing, per DS-1.8 and DS-1.9 • Identify key risks that reflect where the facility believes content losses may occur • Implement and document controls to mitigate or reduce identified risks or where risks are being accepted with rationale (e.g. budget constraints, resource constraints etc.)	Google performs risk assessments as required by ISO/IEC 27001. Google has documented its risk management procedures as part of its ISMS that underlies our ISO/IEC 27001 certification. Documentation is made available to all individuals that may participate in or need to be informed of risk management and assessment programs. See Row PS-5.6 Google conducts rigorous internal continuous testing of our network perimeter through various types of penetration exercises. Google Security Policy prohibits sharing this information but customers may conduct their own testing on our products and services. In addition, Google coordinates external 3rd party penetration testing using qualified and certified penetration testers. The Google security team performs regular testing on systems and processes in addition to audits performed by Google's corporate Internal Audit team that cover multiple disciplines and operational aspects of Google. Google maintains an internal audit program consistent with industry best practices and regulatory requirements.

	• Monitor and assess the effectiveness of remediation efforts and implemented controls at least quarterly • Document and budget for security initiatives, upgrades, and maintenance • Indicate rationale for initiative/project prioritization (risk-based, cost-based, schedule based, etc.) • Consider cyber security insurance (optional) as part of risk mitigation activities. See MS-6.0 for relevance in Business Continuity and Disaster Recovery.	
	III. Security Organization	
MS-3.0	Identify security key point(s) of contact and formally define roles and responsibilities for content and asset protection. Implementation Guidance: • Prepare organization charts and job descriptions to facilitate the designation of roles and responsibilities as it pertains to content security • Provide online or live training to prepare security personnel on policies and procedures that are relevant to their job function	Google has a well established information security organization with well-defined roles and responsibilities, managed by an executive who is dedicated to Security and Privacy, is independent of Information Technology responsibility, and may escalate to the board level concerning security issues. Google's Terms of Service outline the responsibilities of Google and customers Google Cloud roles and responsibilities are reviewed by independent external auditors during audits for our SOC, PCI DSS and ISO/IEC 27001 compliance. Google provides customers (under NDA) a SOC 2 audit report that demonstrates adherence to this control.
	IV. Policies and Procedures	

MS-4.0	Establish policies and procedures regarding asset and content security; policies should address the following topics, at a minimum: ● Acceptable use (e.g., social media, Internet, phone, personal devices, mobile devices, etc.) ● Asset and content classification and handling policies ● Business continuity (backup, retention and restoration) ● Content transfer processes and systems ● 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 ● Storage solutions policy ● Password controls (e.g., password minimum length, screensavers) ● Security policy ● Visitor policy ● Disciplinary/Sanction policy ● Remote and Home Working Policy (WFH) and Procedures ● Internal anonymous method to report piracy or mishandling of content (e.g., telephone hotline or email address) <u>Implementation Guidance:</u> ● Consider facility/business-specific workflows in development of policies and procedures. ● Require executive management to sign off on all policies and procedures before they are published and released ● Communicate disciplinary measures in new hire orientation training ● Please see Appendix D for a list of policies and procedures to consider	Google has well defined policies and procedures regarding asset and content security, the details of which are as follows: Google provides security awareness training to all employees that include reference to our security policies which include our mobile policy. See Row PS-12.0 See Row MS-6.2 Google operates a global network of data centers to reduce risks from geographical disruptions. Google does not depend on failover to other providers but builds redundancy and failover into its own global infrastructure. Google builds multiple redundancies in its systems to prevent permanent data loss. While Google provides IAAS storage capabilities, dealing with business specific requirements is the responsibility of the customer and the storage platform will support the customers requirements. Google embeds redundancy as part of its architecture and failure is expected and corrected continuously. Google annually tests its disaster recovery program which simulates catastrophic events impacting engineering operations. Google performs annual testing of its business continuity plans to simulate disaster scenarios that simulate catastrophic events that may disrupt Google operations. The Google datacenter network infrastructure is secured, monitored, and environmentally controlled.
MS-4.0.1	Establish dedicated policies governing the use of social media by company personnel. <u>Implementation Guidance:</u> ● Social media policies should state that the following not be shared on any social media platform (e.g. Facebook, Twitter, IMDB, YouTube), forum, blog post, or website: ○ Personal experiences, opinions and information related to pre-release content and related project activities ○ References to clients without the express written consent from the client ○ Posting, referencing or sharing of pre-release security or working titles ○ Pre-release content assets or related information without prior authorization	Google has a well established employee communications policy that governs the use of social media.

	• Use separate dedicated email accounts for marketing purposes when accessing social media platforms (e.g. Facebook, Twitter, IMDB, YouTube), forum, blog post, or website.	
MS-4.0.2	Establish policies governing the using of mobile computing devices. Implementation Guidance: • Address the following in mobile computing device policies: ○ BYOD if allowed: define the rights of the company and the rights of the owner, allowable devices / models ○ Acceptable use: corporate and personal ○ Restrictions on areas of the facility where mobile computing devices with recording capabilities are not allowed ○ Procedures for lost or stolen devices ○ Security measures (see Section DS-10)	Google has well established policies governing the use of mobile computing devices. Google provides (under a specific NDA) customers with a SOC 2/3 report that includes compliance of Google's policies governing the use of mobile computing devices.
MS-4.03	Establish, document, communicate, and maintain a policy and procedure to protect content accessed, processed, or stored at remote sites and locations (i.e., Remote and Home Working Policy (WFH) and Procedures). Review the policy and procedure at least annually for updates. Implementation Guidance: Organizations allowing remote working activities (WFH) should issue a policy that defines the conditions and restrictions of working away from a regular office. The following topics should be considered: 1. Remote/WFH workers must sign confidentiality agreements, and others at the location (where local laws allow) 2. Remote/WFH workers must be trained on the Remote and Home Working Policy (WFH) and Procedures, as part of their security awareness training 3. Defining where remote work (WFH) is permitted, and where it is not (e.g., home ok, coffee shop not ok) 4. The method of remote access to the organization's internal systems to perform post-production and/or content creation work. 5. The use of studio approved pixel streaming remote access (such as, PCoIP, RGS, Parsec, NICE DCV, etc.) that restricts processing and content storage on local endpoint devices. 6. Restricting unauthorized access to content from others at the remote working site (i.e., family, friends, and others) 7. Requirements and restrictions for the configuration of wireless network services (Note: wired connection is preferred). 8. Endpoint protection (i.e., local firewall, antivirus, etc.) and network firewall restrictions if they access content locally on the endpoint. 9. The use of multi-factor authentication mechanisms for remote access to the organization's network and/or production network.	Google has policies in place for working remotely and security guidelines which detail the required security and privacy practices for protecting sensitive data while working remotely. Google has processes in place to review Security & Privacy policies annually. The policies for protecting sensitive information at remote locations fall under this category.

	10. The use of encrypted connections for remote access to company networks including the production network 11. Review of remote access users per frequency in MPA Best Practices DS3.2 12. Establish minimum requirements for physical protection of company assets at the remote location Other things to consider: 1. Where feasible encourage the use of corporate owned devices when content is stored locally on the endpoint device 2. Ensure all endpoint devices are patched and updated per frequency in MPA Best Practices (e.g., DS-1.4) 3. Ability to revoke access rights when the remote-working activities are terminated and remote wiping of content from devices through use of MDM and MAM (Mobile device management and Mobile Application Management) (e.g., DS-10.0) 4. Require the return of the equipment, including studio owned assets, once employment is terminated	
MS-4.1	Review and update security policies and procedures at least annually. Implementation Guidance: ● Log/track versions & revisions ● Incorporate the following factors into the annual managerial review of security policies and procedures: ○ Recent security trends ○ Feedback from company personnel ○ New threats and vulnerabilities ○ Recommendations from regulatory agencies (i.e., FTC, etc.) ○ Previous security incidents	See Row PS-11.6 See Row MS-1.3
MS-4.2	Communicate and require sign-off from all company personnel (e.g., employees, temporary workers, interns) and third party workers (e.g., contractors, freelancers, temp agencies) for all current policies, procedures, and/or client requirements. Implementation Guidance: ● Provide the company handbook containing all general policies and procedures upon hire of new company personnel and third party workers ● Notify company personnel and third party workers of updates to security policies, procedures and client requirements ● Management must retain sign-off of current policies, procedures, and client requirements for all company personnel and third party workers	See Row MS-4.3 Google Cloud undergoes periodic compliance audits to validate that employees understand and follow the established policies. Google Cloud roles and responsibilities are reviewed by independent external auditors during audits for our SOC, PCI DSS and ISO/IEC 27001 compliance.

MS-4.3	Develop and regularly update an awareness program about security policies and procedures and train company personnel and third party workers upon hire and annually thereafter on those security policies and procedures, addressing the following areas at a minimum: ● IT security policies and procedures ● Content/asset security and handling in general and client-specific requirements ● Social media policies ● Social engineering prevention ● Security incident reporting and escalation ● Disciplinary policy ● Encryption and key management for all individuals who handle encrypted content ● Asset disposal and destruction processes ● Ransomware ● Work from Home (WFH)/Remote Work security risks. <u>Implementation Guidance:</u> ● Communicate security awareness messages during management/staff meetings ● Implement procedures to track which company personnel have completed their annual security training (e.g., database repository, attendee logs, certificates of completion) ● Provide online or in-person training upon hire to educate company personnel and third party workers about common incidents, corresponding risks, and their responsibilities for reporting detected incidents ● Distribute security awareness materials such as posters, emails, and periodic newsletters to encourage security awareness ● Develop tailored messages and training based on job responsibilities and interaction with sensitive content (e.g., IT personnel, production) to mitigate piracy issues ● Conduct social engineering education, training, and testing (see NIST SP 800-115 and SANS Methods for Understanding and Reducing Social Engineering Attacks) ● Consider recording training sessions and making recordings available for reference ● For additional information on Ransomware refer to NIST SP 1800-26 “Data Integrity Detecting and Responding to Ransomware and Other Destructive Events” ● For WFH/Remote Worker security awareness material, consider referring to SANS Security Awareness Work-from-Home Deployment Kit.” SANS Security Awareness, 2020, www.sans.org/security-awarenesstraining/sans-security-awareness-work-home-deployment-kit	This is primarily a customer responsibility as they own their data. Google provides Google-specific security training. The training is administered online and completion tracked. Completion is required annually. Google personnel are trained on the Data Security policy including procedures for handling customer data. Personnel are required to acknowledge the training they have completed. Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Google’s confidentiality and privacy policies.
	V. Incident Response	

MS-5.0	Establish a formal incident response plan that describes actions to be taken when a security incident is detected and reported. Implementation Guidance: ● Incident response should also cover employees working from home (WFH) and remote workers. ● Consider including the following sections in the incident response plan: ○ Definition of incident ○ Notification of security team ○ Escalation to management ○ Analysis of impact and priority ○ Containment of impact ○ Eradication and recovery ○ Key contact information, including client studio contact information ○ Notification of affected business partners and clients ○ Notification of law enforcement ○ Report of details of incident ● Reference NIST SP800-61 Revision 2 on Computer Security Incident Handling ● Reference the CISA National Cyber Awareness System at: https://uscert.cisa.gov/ncas for information on security alerts, security analysis reports, current threat activity, and vulnerability bulletins and additional templates for incident reporting at https://us-cert.cisa.gov/report	Google operates a global network of data centers to reduce risks from geographical disruptions. The locations of our data centers can be found here. Google does not depend on failover to other providers but builds redundancy and failover into its own global infrastructure. Google performs annual testing of its business continuity plans to simulate disaster scenarios that simulate catastrophic events that may disrupt Google operations. Google monitors a variety of communication channels for security incidents, and Google's security personnel will react promptly to known incidents. Se Row MS-5.1 See Row DS-9.3
MS-5.1	Identify the security incident response team who will be responsible for detecting, analyzing, and remediating security incidents. Implementation Guidance: ● Include representatives from different business functions in order to address security incidents of all types; consider the following: ○ Management ○ Physical security ○ Information security ○ Network team ○ Human resources ○ Legal ● Provide training so that members of the incident response team understand their roles and responsibilities in handling incidents	Google has a well defined and rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Google's security incident management program is structured around the NIST guidance on handling incidents (NIST SP 800–61). Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Google requires its employees to report immediately, all known or suspected information security and privacy incidents (defined as "Data Incidents" below) to the Security and Privacy Incident Management team. For more details, refer to section 7.2 of Google's Cloud Data Processing Addendum. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Additionally, Google communicates outage information through its status dashboards: ● For Google Cloud ● For Google Workspace Due to the fact that the incident response system is standardized, customization of the notification process is not supported for each tenant. The terms of service cover roles and responsibilities.

		Google performs annual testing of its emergency response processes. Google's end-to-end data incident response process is described in this whitepaper.
MS-5.2	Establish a security incident reporting process for individuals to report detected incidents to the security incident response team. Implementation Guidance: • Consider implementing a group email address for reporting incidents that would inform all members of the incident response team • Communicate and document 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. • Implement a security breach notification process, including the use of breach notification forms • Involve the Legal team to determine the correct actions to take for reporting content loss to affected clients • Discuss lessons learned from the incident and identify improvements to the incident response plan and process • Perform root cause analysis to identify security vulnerabilities that allowed the incident to occur • Identify and implement remediating controls to prevent similar incidents from reoccurring • Communicate the results of the post-mortem, including the corrective action plan, to affected clients	See Row MS-5.1
MS-5.2.1	Anonymous reporting should be made available to organizations with 50 or more employees and third party personnel for reporting of content protection and piracy concerns. The anonymous reporting tool consisting of an internal, anonymous telephone number, email address, and / or website should be published and also provided during security awareness training.	See Row MS-5.1
MS-5.3	(Removed and combined with MS-5.2)	
	VI. Business Continuity and Disaster Recovery	
MS-6.0	Establish a formal plan that describes actions to be taken to ensure business continuity. Implementation Guidance: Consider including the following sections in the business continuity plan: • Threats to critical assets and content, including loss of power and telecommunications, systems failure, natural disasters etc. • Consider cyber security insurance (optional) to help mitigate risks from a cyberattack including, but not limited to: (1) identity theft; (2) business interruption; (3) damage to reputation; (4) data repair costs; (5) theft of	Google operates a global network of data centers to reduce risks from geographical disruptions. Locations of our data centers can be found here. Google does not depend on failover to other providers but builds redundancy and failover into its own global infrastructure. Google has implemented redundancies and safeguards in its data centers to minimize the impact of service outages. Google builds multiple redundancies in its systems to prevent permanent data loss. All files are replicated at least three times and to at least two data centers. Google embeds redundancy as part of its architecture and failure is expected and corrected continuously. Google annually tests its disaster recovery program which simulates catastrophic events impacting engineering operations.

	customer lists or trade secrets; (6) hardware and software repair costs; (7) credit monitoring services for impacted consumers; and (8) litigation costs. • The plan should also cover remote workers, and work from home (WFH) employees, and business functions that are occurring remotely. Risks unique to working remotely should be documented and addressed in the business continuity plan. • Detailed information system, content and metadata backup procedures and information system documentation, including configuration of critical WAN and LAN / Internal Network devices • Encryption of backups (AES-256) • Backup power supply to support at least 15 minutes for the surveillance camera system, alarm and critical information systems, including software to perform a safe shutdown of critical systems • Consider use of an off-site backup location • Notification of security team • Escalation to management • Analysis of impact and priority • Containment of impact • Priorities for recovery and detailed recovery procedures, including manual workarounds and configuration details of restored systems • Key contact information • Notification of affected business partners and clients • Testing of business continuity and disaster recovery processes at least annually	Google performs annual testing of its business continuity plans to simulate catastrophic events that may disrupt Google operations. The Google datacenter network infrastructure is secured, monitored, and environmentally controlled. Customers can define the zone or region that data is available, but they may not define if it is transported through a given legal jurisdiction. Google provides documentation to customers to develop failover mechanisms for their environment. Failover to other providers is customer responsibility. See Row MS-6.2 See Row PS-9.1
MS-6.1	Identify the business continuity team who will be responsible for detecting, analyzing and remediating continuity incidents. Implementation Guidance: • Include defined roles and responsibilities • Provide training so that members of the business continuity team understand their roles and responsibilities	Engineering teams maintain playbooks to facilitate the rapid reconstitution of services.
MS-6.2	Establish a data backup policy that addresses the following: • Systems and data • Retention and protection requirements • Backup frequency • Encryption • Recovery time objectives (RTO) • Recovery point objectives (RPO) • Restoration testing • Secure offsite storage Implementation Guidance: • Align backup policy with the business continuity plan	Google has documented policies and procedures governing data retention periods that are routinely reviewed and updated. While Google provides IAAS storage capabilities, dealing with business specific requirements is the responsibility of the customer and the storage platform will support the customers requirements. Many Cloud products allow customers to choose their geographic location, this setting is configured when the service is first set up and is covered by the service specific terms. Google may store customer data in the following locations. Customers can define the zone or region that data is available, but they may not define if it is transported through a given legal jurisdiction. Discover our data center locations here. Customers retain control and ownership over their content. Customers are responsible for managing their data retention policies. Customers may leverage the features of our storage services. Refer to product documentation for specifics.

	• Implement physical and environmental security controls (per MPA guidelines) for offsite storage to prevent unauthorized access or stolen / lost content
	• Encrypt backups using AES with at least 256 bit key before storing content offsite in remote locations or on the cloud
	• Notify clients if the cloud backups will be used
	• Frequency of backups and recovery testing must be based on RTO and RPO that meets client requirements. The following is recommended:
	  ○ Daily incremental and weekly backups
	  ○ RTO of 48 hours or less for client content
	  ○ Quarterly data restoration testing
	• Review process should be in place to ensure that only authorized administrators are able to access backup location	

	VII. Change Control & Configuration Management	

MS-7.0	Establish policies and procedures to ensure new data, applications, network, and systems components have been pre-approved by business leadership.
	
	Implementation Guidance:
	• Include documentation that describes installation, configuration and use of devices, services and features, and update documentation as needed
	• Document known issues and procedures for dealing with them
	• Include procedures for reporting bugs and security vulnerabilities
	• Restrict and monitor the installation of hardware or software
	• Manage risks associated with changes to data, applications, network infrastructure and systems
	  ○ Review security controls and integrity procedures to ensure they will not be compromised by changes
	  ○ Ensure that appropriate backup or roll-back procedures are documented and tested
	  ○ Identify all affected computer software, data files, database entities, and infrastructure
	  ○ Minimize business disruption when implementing change
	• Document and retain all change requests, testing results and management approvals
		The authorization to provision additional processing capacity is obtained through budget approvals and managed through internal SLAs as part of an effective resource economy. Refer to our documentation and learning center for more details.
		
		See Row DS-1.12
		
		See Row DS-6.8
		
		Google's native authentication requires a minimum 8 character complex password.
		Tenants can set the maximum or increase the minimum. A built-in Password Monitor is visible to the end user upon password creation and to the System Administrators of the tenant who can decide to force a password change on any user that is later detected to have a password that is weak. Google's native authentication has protections in place that would detect a brute force attack and challenge the user to solve a Captcha and would auto lock the account if suspicious activity is detected. The tenant's System Administrators can reset that account for the end user.

	VIII. Workflow	

MS-8.0	Document workflows tracking content and authorization checkpoints. Include the following processes for both physical and digital content: • Delivery (receipt/return) • Ingest • Movement • Storage • Removal/destruction Implementation Guidance: • Use swim lane diagrams to document workflows • Include asset processing and handling information where applicable • Evaluate each touch-point for risks to content • Implement controls around authorization checkpoints • Identify related application controls • Update the workflow when there are changes to the process, and review the workflow process at least annually to identify changes. • Follow the content workflow and implemented controls for each process in order to determine areas of vulnerability	Google provides (under a specific NDA) customers with a SOC 2/3 report that demonstrates compliance with this requirement.
MS-8.1	(Removed and combined with MS-8.0)	
	IX. Segregation of Duties	

MS-9.0	Segregate duties within the content workflow. Implement and document compensating controls where segregation is not practical.
	
	Implementation Guidance:
	• Document roles and responsibilities to eliminate an overlap of role-based job functions such as:
	  ○ Vault and server/machine room personnel
	  ○ Shipping and receiving personnel
	  ○ Asset movement within facility (e.g., runners) from vault and content / production area
	  ○ Digital asset folder access (e.g., data wrangler sets up access for producer)
	  ○ Content transfer personnel from production personnel
	• Segregate duties using manual controls (e.g., approval from producer before working on content) or automated controls in the work ordering system (e.g., automated approval for each stage of the workflow)
	• Implement compensating controls when segregation is unattainable, such as:
	  ○ Monitor the activity of company personnel and/or third party workers
	  ○ Retain and review audit logs
	• Implement physical segregation
	• Enforce management supervision
		Google restricts access based on need-to-know and job functions. Google maintains automated log collection and analysis tools.
		
		See Row PS-15.2
		
		Google's production environment is segregated from our corporate environment. Multi-factor authentication is required for any connections to our production environment.
		
		See Row PS-16.4
		
		Google follows a structured code development and release process. As part of this process, code is peer reviewed. Google makes proprietary code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats.

	X. Background Checks	

MS-10.0	Perform background screening checks on all company personnel, third party workers, and their relevant subcontractors. Implementation Guidance: • Carry out background checks in accordance with relevant laws, regulations, union bylaws, and cultural considerations • Screen potential company personnel and third party workers using background screening checks that are proportional to the business requirements, the sensitivity of content that will be accessed, and possible risks of content theft or leakage • Perform identity, academic, and professional qualification checks where necessary • Where background checks are not allowed by law, document as an exception and use reference checks	Google conducts reasonably appropriate background checks on all its employees to the extent legally permissible and in accordance with applicable local labor law and statutory regulations. For further information on employee onboarding and security and privacy training, refer to our Security White Paper.
	XI. Confidentiality Agreements	
MS-11.0	Require all company personnel to sign a confidentiality agreement (e.g., non-disclosure) upon hire and review annually thereafter, that includes requirements for handling and protecting content. Implementation Guidance: • Confidentiality agreements must also be signed by remote workers and personnel working from home (WFH). Confidentiality agreements should also be considered for other members of the household (e.g., roommate, spouse, etc.) at the remote location, who could potentially be exposed to content, where local laws allow • Include non-disclosure guidance pertaining to confidentiality after termination of their employment, contract, or agreement • Explain the importance of confidentiality / NDA in non-legal terms, as necessary • Ensure all relevant information on equipment used by company personnel to handle business-related sensitive content is transferred to the organization and securely removed from the equipment • Management must retain signed confidentiality agreements for all company personnel	Google reviews NDA and confidentiality documents as needed. All Google employees are required to sign a non disclosure agreement as part of the hiring application prior to joining the company.

MS-11.1	Require all company personnel to return all content and client information in their possession upon termination of their employment or contract. Implementation Guidance: Utilize an off boarding process for terminated employees to ensure the following: ● all content and client information is returned ● company equipment and property is returned ● keys, access cards, badges are returned ● reasons for termination are documented ● user accounts / access rights on all systems are removed or disabled ● Documenting and storing a history of terminated personnel for five years at a minimum ● Formally reminding departing personnel of their ongoing confidentiality and non-disclosure responsibilities	Google has a well defined exit process including equipment return procedures for terminated employees and third party workers. Access to production machines, support tools, network devices and corporate assets is automatically removed on a timely basis upon submission of a termination request by Human Resources or a manager. Google is able to track all devices via a centrally managed system.
	XII.Third Party Use and Screening	
MS-12.0	Require all third party workers (e.g., freelancers) who handle content to sign confidentiality agreements (e.g., non-disclosure) upon engagement. Implementation Guidance: ● Include non-disclosure guidance in policies pertaining to confidentiality during and after their employment, contract, or agreement ● Explain the importance of confidentiality / NDA in non-legal terms, as necessary ● Ensure all relevant information on equipment used by third party workers to handle business-related sensitive content is transferred to the organization and securely removed from the equipment ● Management must retain signed confidentiality agreements for all third party workers ● Include requirements for handling and protecting content	Google has well established agreements including non-disclosure agreements for preserving the confidentiality of information and software exchanges with external parties. All third party personnel are required to sign a NDA prior to engaging their services with the company. See Row MS-11.0
MS-12.1	Require all third party workers to return all content and client information in their possession upon termination of their contract.	See Row MS-11.1
MS-12.2	Include security requirements in third party contracts. Implementation Guidance: ● Service Level Agreements (SLAs) and contracts with the third party vendors should the following provisions: ○ Require third party workers to comply with the security requirements per MPA Best Practices ○ A right to audit clause for activities that involve sensitive content ○ Notification to clients upon suspected or actual security breaches ○ Content ownership, return, and destruction ○ Termination clause ● Implement a process to monitor for compliance with security requirements ● Require annual update of information when contracts are renewed	Google employs a vendor management process that includes contractual requirements to adhere to Google's security policies and onsite inspections, as needed, to confirm compliance.

MS-12.3	Implement a process to reclaim content when terminating relationships with third party service providers. Implementation Guidance: ● Ensure all content on third party equipment is transferred to the organization and securely erased from the equipment	See Row MS-11.1
MS-12.4	Require third party workers to be bonded and insured where appropriate (e.g., courier service). Implementation Guidance: ● Require third party workers to show proof of insurance and keep a record of their insurance provider and policy number ● Require annual update of information when contracts are renewed	Google employs a vendor management process that includes contractual requirements to adhere to Google's security policies and onsite inspections, as needed, to confirm compliance.
MS-12.5	Restrict third party access to content / production areas unless required for their job function. Implementation Guidance: ● Ensure that third party workers who do not handle content (e.g., cleaning crews, HVAC maintenance, etc.) are not given any access to areas housing or exhibiting content ● Escort third party workers who do not handle content when access to restricted areas (e.g., vault) is required	See Row PS-4.0 See Row PS-15.4 See Row PS-1.1 See Row DS-1.6
MS-12.5.1	Control access of third party IT service providers to the computing environment. Implementation Guidance: ● Third-party VPN remote access should only be used in cases where no other solution is available. ● Client approval is required in writing. ● All third-party VPN remote access should have a finite end date and be reviewed for activity every three months at a minimum ● Third-party VPN remote access should not provide access to network infrastructure that includes networks or systems used to store, transfer, or manipulate content ● All third-party access sessions should be monitored by an employee and logged ● Log and monitor IT service providers access to systems, networks, and infrastructure ● Third-party systems used for remote access should be subjected to an inspection, by an employee, on a periodic and ongoing basis IT service provider remote access must utilize multi-factor authentication ● Disable IT service provider remote access when not needed ● Change remote access passwords for every session ● Follow change control processes for elevating user access rights ● Consider real-time notification when IT service providers access systems	See Row PS-4.0 See Row PS-15.4 See Row PS-1.1 See Row DS-1.6

MS-12.6	Notify clients if third parties are used to handle or store content, or work is offloaded to another company. Perform due diligence of third parties. Third parties also include providers of IT services. Obtain client approval for use of third parties who handle, store, or have access to content. Implementation Guidance: ● Work offloaded to another company must be reported to the content owners and requires written client sign-off / approval ● Production servers and systems hosted on third-party networks must be vetted by content owners prior to deployment. ● Cloud-Hosted systems and servers are strictly prohibited without advanced written consent of content owners. ● Workflows using cloud hosted servers should be approved by content owners ● Perform due diligence and ongoing monitoring of third parties to verify the following: ○ Security controls meet MPA Best Practices ○ Adequate level of insurance coverage (refer to MS12.4) ○ Viable financial state ● Request that third parties obtain an independent security assessment for submission to the member studios ● Cloud providers and/or data center providers should have a valid SOC2, ISO 27001 or AOC (PCI) or equivalent audit report which covers cloud infrastructure and/or data center services.	Google has a well defined vendor management policy and process to select and monitor third party providers. Google conducts ongoing audits of its third party subprocessors for compliance. Google requires its third party subprocessors to meet the same high standards that it does. In particular, Google requires its third party subprocessors to comply with its contract with companies and applicable law and regulation. To enable companies to retain oversight of any third party subprocessors and provide choices about the services that companies use, Google will: ● provide information about its subprocessors (at least 30 days before the new subprocessor begins processing company data) ● provide advance notice of changes to its subprocessors; and ● give companies the ability to terminate if they have concerns about a new subprocessor. Refer to the Cloud Data Processing Addendum section on subprocessors for more details.
	XIII. Entry/Exit Points	
PS-1.0	Secure all entry/exit points of the facility at all times, including loading dock doors and windows. Implementation Guidance: ● For remote workers working from home or a remote facility, entry/exit points to the location should have the ability to be secured. ● For remote workers consider blinds/window shades where content could be visible from the outside ● Permit entry / exit points to be unlocked during business hours if the reception area is segregated from the rest of the facility with access-controlled doors ● Entry/exit points at a facility server room, datacenters, colocations, and cloud hosting facilities where content is stored, must be secured. Proof can be provided via valid SOC2, ISO 27001, AOC (PCI), or any equivalent audit report covering physical security	See Row PS-4.0 See Row PS-15.4

PS-1.1	Control access to areas where content is handled by segregating the content area from other facility areas (e.g., administrative offices, waiting rooms, loading docks, courier pickup and drop-off areas, replication and mastering). Implementation Guidance: ● For remote workers (WFH), segregated work areas do not apply when a segregated area for content handling is not available, such as a small apartment or studio ● Allow access to content / production areas on a need-to know basis ● Require rooms used for screening purposes to be access controlled (e.g., projection booths) ● Limit access into rooms where media players are present (e.g., Blu-ray, DVD) ● Enforce a segregation of duties model which restricts any single person from having access to both the replication and mastering rooms	Google maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors, and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request (which is followed by proper approval process) electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and requires the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations (iii) and reference an approved data center access record identifying the individual as approved. All visitors are badged using a centralized controlled and monitored system. Google requires all visitors to sign a NDA and a visitor log prior to entry, and requires all visitors to be escorted at all times.
PS-1.2	Control access where there are collocated businesses in a facility, which includes but is not limited to the following: ● Segregating work areas ● Implementing access-controlled entrances and exits that can be segmented per business unit ● Logging and monitoring of all entrances and exits within facility ● All tenants within the facility must be reported to client prior to engagement	Google maintains a physical security policy that describes the requirements for maintaining a safe and secure work environment. Google trains its employees and contractors annually in its security policies. Third-parties agree to observe Google's security policies as part of their contract.
	XIV. Visitor Entry/Exit	
PS-2.0	Maintain a detailed visitors' log and include the following: ● Name ● Company ● Time in/time out ● Reason for visit ● Person/people visited ● Signature of visitor ● Badge number assigned Implementation Guidance: ● Verify the identity of all visitors by requiring them to present valid photo identification (e.g., driver's license or government-issued ID) ● Consider concealing the names of previous visitors ● The facility should retain visitor logs for twelve months at a minimum or the maximum duration allowed by local privacy laws.	Google maintains a central identity and authorization management system.
PS-2.1	Assign an identification badge or sticker which must be visible at all times, to each visitor and collect badges upon exit.	All visitors are badged using a controlled, centralized and monitored system.

	Implementation Guidance: • Make visitor badges easily distinguishable from company personnel badges (e.g., color coded plastic badges) • Consider a daily rotation for paper badges or sticker color • Consider using badges that change color upon expiration • Log badge assignments upon entry/exit • Visitor badges should be sequentially numbered and tracked • Account for badges daily • Facilities that have less than 25 employees are not required to have visitor badges	
PS-2.2	Do not provide visitors with key card access to content / production areas.	See Row PS-1.1
PS-2.3	Require visitors to be escorted by authorized employees while on-site, or in content / production areas.	See Row PS-1.1
PS-2.3.1	Visitors should be required to sign a nondisclosure agreement (NDA) and sign a visitor log prior to entering a facility.	See Row PS-1.1
	XV. Identification	
PS-3.0	For organizations with 25 or more employees and third-party workers, 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 Implementation Guidance: • Issue photo identification badge to all company personnel and long-term third party workers after a background check has been completed • Establish and implement a process for immediately retrieving photo identification badge upon termination • Consider omitting location, company name, logo and other specific information on the photo identification badge • Consider using the photo identification badge as the access key card where possible • Require employees to immediately report lost or stolen photo identification badges • Provide a 24/7 telephone number or website to report lost or stolen photo identification badges • Train and encourage employees to challenge persons without visible identification	All employees and contractors are given specially printed photo ID badges and must wear them visibly at all times. See Row PS-1.1
	XVI. Perimeter Security	
PS-4.0	Implement perimeter security controls that address risks that the facility may be exposed to as identified by the organization's risk assessment. Implementation Guidance:	Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control systems that are linked to a system alarm. Access to perimeter doors, shipping and receiving, and other critical areas is logged, including unauthorized activity. Failed access attempts are logged by the access control system and investigated as appropriate. Authorized access throughout the business operations and data centers is

	• Implement security controls based upon the location and layout of the facility, such as: ○ Restricting perimeter access through the use of walls, fences, and/or gates that, at a minimum, are secured after hours; walls/fences should be 8 feet or higher ○ Securing and enclosing, as necessary, common external areas such as smoking areas and open balconies ○ Installing lighting with full coverage outside the facility to decrease risk of theft or security violations ○ Sufficient external camera coverage around common exterior areas (e.g., smoking areas), as well as parking ○ Being cognizant of the overuse of company signage that could create targeting ○ Glass break sensors as necessary ○ Using alarms around the perimeter, as necessary	restricted based on an individual's job responsibilities. The fire doors at the data centers are alarmed and can only be opened from the inside. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to help cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. Security operations personnel manage the CCTV monitoring, recording and control equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. Refer to the following resources for further information: • Appendix 2 of Google's Cloud Data Processing Addendum describe the security measures that Google will implement and maintain • Google Cloud Security White Paper for details on our data center security
PS-4.1	Place security guards at perimeter entrances and nonemergency entry/exit points. Implementation Guidance: • **Note**: Not all sites require security guards. This should be determined based on risk, per MS-2.1	See Row PS-4.0
PS-4.2	Implement a daily security patrol process with a randomized schedule and document the patrol results in a log. Implementation Guidance: Consider the following if applicable: • Require security guards to patrol both interior and exterior areas • Include a review of emergency exits, including verification of seals • Use a guard tour patrol system to track patrolling (e.g., checkpoint) and verify locks	Physical security personnel patrol all Google work areas and data centers.
PS-4.3	Lock perimeter gates at all times. Implementation Guidance: Consider the following if applicable: • Implement an electronic arm, that is manned by security personnel, to control vehicle access into the facility • Distribute parking permits to company personnel and third party workers who have completed the proper paperwork • Require visitor vehicles to present identification and ensure that all visitors have been pre-authorized to enter the premises	See Row PS-4.0
	XVII. Alarms	

PS-5.0	Install a centralized, audible alarm system that covers all entry/exit points (including emergency exits), windows, loading docks, fire escapes, and restricted areas (e.g., vault, server/machine room, etc.). Implementation Guidance: • Place alarms at every entrance to alert security personnel upon unauthorized entry to the facility • Enable the alarm when facility is unsupervised • Remote and work from home (WFH) locations where physical content is handled onsite, should consider an alarm system. • Where content is stored at a facility server room, datacenters, colocations, and cloud hosting facilities and used as part of remote working they must include an alarm system. Proof can be provided via a valid SOC2, ISO 27001, AOC (PCI), or any equivalent audit report covering physical security that includes an alarm system.	See Row PS-4.0 See Row PS-15.4
PS-5.1	Install and effectively position motion detectors in restricted areas (e.g., vault, server/machine room) and configure them to alert the appropriate security and other personnel (e.g. project managers, producer, head of editorial, incident response team, etc.). Implementation Guidance: • Ensure the alarm system covers storage areas and vaults (e.g., through motion sensors) after normal business hours, as an added layer of security	See Row PS-4.0 See Row PS-15.4
PS-5.2	Install door prop alarms in restricted areas (e.g. vault, server, machine rooms) to notify when sensitive entry/exit points are open for longer than a predetermined period of time (e.g., 60 seconds). Implementation Guidance: • Configure access-controlled doors to trigger alarms and alert security personnel when doors have been propped open for an extended period of time	See Row PS-4.0
PS-5.3	Configure alarms to provide escalation notifications directly to the personnel in charge of security and other personnel (e.g., project managers, producer, head of editorial, incident response team, etc.). Implementation Guidance: • Establish and implement escalation procedures to be followed if a timely response is not received from security personnel upon notification • Consider implementing automatic law enforcement notification upon breach • Implement procedures for notification on weekends and after business hours	See Row PS-4.0
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. Implementation Guidance:	Google maintains a central identity and authorization management system.

	• Use unique alarm codes to track individuals responsible for arming or disarming the alarm • Update assigned alarm codes at an interval approved by management in order to reduce risk involved with sharing and losing codes • Issue alarm codes to personnel on a least privilege basis • Security personnel, contractors, vendors, cleaning crews, and freelance staff should not have administrator rights to the alarm system • Alarm notifications should be sent to appropriate company personnel according to an escalation tree.	
PS-5.5	Review the list of users who can arm and disarm alarm systems quarterly, or upon change of personnel. Implementation Guidance: • Remove users who have left the company or have changed job roles • Deactivate the alarm codes that were assigned to removed users	See Row PS-15.2 See Row PS-16.4 See Row PS-6.2

PS-5.6	Test the alarm system quarterly
	
	Implementation Guidance:
	• Simulate a breach in physical security and ensure the following:
	  ○ Alarm system detects the breach
	  ○ Security personnel are alerted
	  ○ Security personnel respond in a timely manner according to procedures
		Google performs periodic network vulnerability scans, application-layer vulnerability scans, local operating system-layer scans and checks using commercial and proprietary tools.
		
		Google does not make vulnerability scan results available to customers but customers can perform their own scans. Google files bug tickets for any identified issues that require remediation. Bug tickets are assigned a priority rating and are monitored for resolution.
		
		Google operates a homogeneous machine environment with custom software to minimize exposure to vulnerabilities in commercial products and to allow rapid patching if needed. Google currently patches systems as needed and as quickly as vulnerabilities are addressed rather than on a scheduled basis.
		
		The notification process is determined in the terms of service and security whitepaper.
		
		More information about reporting security issues can be found here.
		
		Google Cloud provides the ability to log and monitor security and system health.

PS-5.7	Implement fire safety measures so that in the event of a power outage, fire doors fail open, and all others fail shut to prevent unauthorized access.	See Row PS-4.0
	XVIII. Authorization	
PS-6.0	Document and implement a process to manage facility access and keep records of any changes to access rights. Implementation Guidance: • Designate an individual to authorize facility access • Notify appropriate personnel (e.g., facilities management) of changes in employee status • Create a physical or electronic form that must be filled out by a supervisor to request facility access for company personnel and/or third party workers	See Row PS-15.2 See Row PS-16.4

	• Assign responsibility for investigating and approving access requests.	
PS-6.1	Restrict access to production systems to authorized personnel only.	Customers can provision separate domains or organizations with a domain for testing purposes. Google provides solution papers and reference Development and Test environments. Google segregates its production environment from its corporate environment. Google Cloud has been validated and certified by independent external auditors to confirm alignment with SOC 2/3 controls (section CC6.1 #64) for network segmentation. Google provides customers (under NDA) SOC 2 report that shows compliance with these controls.
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. Implementation Guidance: • Validate the status of company personnel and third party workers • Remove access rights from any terminated users • Verify that access remains appropriate for the users' associated job function	Google requires access reviews at least annually for critical access groups. Google logs all changes in user permissions. Google revokes access when no longer required. Google notifies customers of security incidents that impact their data and will work with the customer in good faith to address any known breach of Google's security obligations. Google provides (under a specific NDA) customers with a SOC 2/3 report that includes testing of Google's access controls. Details are documented in the Google Cloud Security White Paper.
	XIX. Electronic Access Control	
PS-7.0	Implement electronic access throughout the facility to cover all entry/exit points and all areas where content is stored, transmitted, or processed. Implementation Guidance: • Assign electronic access to specific facility areas based on job function and responsibilities • Update electronic access accordingly when roles change or upon termination of company personnel and third party workers • Keep a log that maps electronic access device number to company personnel • See Logging and Monitoring PS-10.0 • Review the times when electronic access is not required for common areas (e.g., public elevators)	See Row PS-4.0
PS-7.1	Restrict electronic access system administration to appropriate personnel. Implementation Guidance: • Restrict electronic system administration to designated personnel and do not allow individuals who have access to production content to perform administrative electronic access tasks • Assign an independent team to administer and manage electronic access	See Row PS-4.0
PS-7.2	Store card stock and electronic access devices (e.g., keycards, key fobs) in a locked cabinet and ensure electronic access devices remain disabled prior to being assigned to personnel. Store unassigned electronic access devices (e.g., keycards, key fobs) in a locked cabinet and ensure these remain disabled prior to being assigned to personnel.	See Row PS-4.0

	Implementation Guidance: • Limit access to the locked cabinet to the keycard / electronic access device system administration team • Require sign-out for inventory removal	
PS-7.3	Disable lost electronic access devices (e.g., keycards, key fobs) in the system before issuing a new electronic access device. Implementation Guidance: • Educate company personnel and third party workers to report lost electronic access devices immediately to prevent unauthorized access into the facility • Require identification before issuing replacement electronic access devices	See Row PS-4.0
PS-7.4	Issue third party access electronic access devices with a set expiration date (e.g. 90 days) based on an approved timeframe. Implementation Guidance: • Ensure that third party electronic access devices are easily distinguishable from company personnel electronic access devices • Ensure that expiration date is easily identifiable on the electronic access devices • Assign third party electronic access devices on a need-to know basis	See Row PS-4.0
	XX. Keys	
PS-8.0	Limit the distribution of master keys and / or keys to restricted areas to authorized personnel only (e.g., owner, facilities management). Implementation Guidance: • Physical keys should not unlock entryways to override electronic access control to restricted areas (e.g., vault, server, or machine rooms). If they do, an alarm should be triggered • Maintain a list of company personnel who are allowed to check out master keys • Update the list regularly to remove any company personnel who no longer require access to master keys • Monthly inventory checks of physical keys and master keys should be conducted • Unassigned keys should be stored in a safe location (e.g., lockbox or safe)	See Row PS-4.0

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.
	
	Implementation Guidance:
	• Maintain records to track the following information:
	  ○ Company personnel in possession of each master key
	  ○ Time of check-out/check-in
	  ○ Reason for check-out
		See Row PS-4.0

	• Require master keys to be returned within a set time period and investigate the location of keys that have not been returned on time	

PS-8.2	Use keys that can only be copied by a specific locksmith for exterior entry/exit points.
	
	Implementation Guidance:
	• Use high-security keys (cylinders) that offer a greater degree of resistance to any two or more of the following:
	  ○ Picking
	  ○ Impressioning
	  ○ Key duplication
	  ○ Drilling
	  ○ Other forms of forcible entry
		See Row PS-4.0

PS-8.3	Inventory master keys and keys to restricted areas, including facility entry/exit points, quarterly. Implementation Guidance: • Identify, investigate, and address any missing keys (lost/stolen) • Review logs to determine who last checked out a key that cannot be accounted for • Change the locks when missing master keys or keys to restricted areas cannot be accounted for	See Row PS-4.0
PS-8.4	Obtain all keys from terminated employees/third-parties or those who no longer need the access.	See Row MS-11.1
PS-8.5	Implement electronic access control or rekey the entire facility when master or sub-master keys are lost or missing.	See Row PS-4.0
	XXI. Cameras	
PS-9.0	Install a surveillance camera system (analog CCTV or IP cameras) that records all facility entry/exit points and restricted areas (e.g. server/machine room, etc.). Implementation Guidance: • Camera cables and wiring should be discreetly hidden from view and not within reasonable reach • Facility should not assume that cameras provided by the building are adequate • Place cameras at every entrance / exit to the facility • Ensure the cameras cover storage areas and vaults • Cameras in server / machine rooms should cover both the front and back of the racks • Use rack mounted cameras to provide coverage of the ports of computing equipment where content resides; this applies to instances where other cameras have an obscured view of the ports (e.g., equipment housed at colocation data centers.)	See Row PS-4.0

	• Camera surveillance systems should be considered for WFH/remote worker locations	
PS-9.1	Review camera positioning and recordings to ensure adequate coverage, function, image quality, lighting conditions, and frame rate of surveillance footage at least daily. Implementation Guidance: • Position cameras to ensure an unobstructed view of all entry/exit points and other sensitive areas • Position and orient cameras to capture facial features that might be partially obstructed by hats, hoods, or other worn headgear • Accommodate for cameras in dark areas (e.g., low-light or infrared cameras, motion-detecting lights) • Implement sufficient image quality and lighting to ensure that faces are distinguishable. Record with sufficient resolution to identify facial features • Set frame rate to ensure that activity is adequately recorded. Record at a minimum rate of 7 frames per second • Position and orient cameras to avoid capturing content on display • Where local privacy laws restrict implementation of these recommendations, modifications may be made with a reference to the specific law.	Google anticipates physical threats to its data centers and has implemented countermeasures to prevent or limit the impact from these threads. This video provides an overview of our countermeasures: Refer to the following resources for further information: • Appendix 2 of Google's Cloud Data Processing Addendum describe the security measures that Google will implement and maintain • Google Cloud Security White Paper for details on our data center security • Information on Data Center Security
PS-9.2	Restrict physical and/or logical access to the surveillance camera console and camera equipment (e.g., DVRs, NVRs) to personnel responsible for administering/monitoring the system Implementation Guidance: • Place camera equipment in a secure access controlled location (e.g., computer room, locked closet, cage) • Perform periodic access reviews to ensure that only the appropriate individuals have access to surveillance equipment • Ensure that the web console for IP-based adheres to the following: 1. camera system is restricted to authorized personnel 2. Strong account management controls are in place (e.g., password complexity, individual user login, logging and monitoring) 3. Consider restricting administrative access to the local LAN only 4. Consider enabling Multi-Factor Authentication (MFA) for access to the camera system 5. Camera footage should be stored locally. Client approval must be obtained if cloud storage of footage is being considered 6. The camera system should be restricted to its own dedicated LAN and connections from this LAN to the networks that handle content should not be allowed	Google restricts access based on need-to-know and job functions. Google maintains automated log collection and analysis tools. Multi-factor authentication is required for any connections to our production environment. Google maintains a central identity and authorization management system. See Row PS-16.4
PS-9.3	Ensure that camera footage includes an accurate date and time-stamp and retain camera surveillance footage and electronic access logs for at least 90 days, or the maximum time allowed by law, in a secure location.	See Row PS-9.1

	Implementation Guidance: • Burn the time and date onto the physical media for camera footage recorded on tape or disk • Ensure that accurate time-stamps are maintained on the recording equipment for digital camera footage • Review date and time stamp for accuracy at least weekly • Consider storing logs in an access-controlled telecom closet or computer room • Determine the typical amount of space required for one day of logging and ensure that the log size is large enough to hold records for at least 90 days, or the maximum retention period allowed by law • Consider retaining camera surveillance footage until the first production release date	
PS-9.4	Designate an employee or group of employees to monitor surveillance footage during operating hours and immediately investigate detected security incidents. Implementation Guidance: • Incorporate the incident response process for handling security incidents • Consider adding a surveillance monitor at the reception desk or in the IT office	See Row PS-9.1
	XXII. Logging and Monitoring	

PS-10.0	Log and review electronic access to restricted areas for suspicious events, at least weekly.
	
	Implementation Guidance:
	• Identify and document a set of events that are considered suspicious
	• Consider the implementation of an automated reporting process that sends real-time alerts to the appropriate security personnel when suspicious electronic access activity is detected
	• Retain logs for one year, at a minimum
	• Log and review the following events:
	  ○ Repeated failed access attempts
	  ○ Unusual time-of-day access
	  ○ Successive door access across multiple zones
		See Row PS-9.1

PS-10.1	Log and review electronic access, at least daily, for the following areas: • Masters/stampers • vault • Pre-mastering • Server/machine room • Scrap room • High-security cages. Implementation Guidance: • Identify and document events that are considered unusual	See Row PS-9.1

	• Consider the implementation of an automated reporting process that sends real-time alerts to the appropriate security personnel when suspicious electronic access activity is detected	
PS-10.2	Investigate suspicious electronic access activities that are detected. Implementation Guidance: • Identify and communicate key contacts that should be notified upon detection of unusual electronic access activity • Establish and implement escalation procedures that should be followed if primary contacts do not respond to event notification in a timely manner	Google machine configuration changes are continuously monitored when online. Google Cloud provides the ability to log and monitor the health of virtual instances using a variety of tools. Refer here for documentation.
PS-10.3	Maintain an ongoing log of all confirmed electronic access incidents and include documentation of any follow-up activities that were taken. Implementation Guidance: • Leverage the incident response reporting form to document confirmed keycard / electronic access device incidents • Review all recent keycard / electronic access device incidents periodically and perform root-cause analysis to identify vulnerabilities and appropriate fixes	Google reviews and analyzes security incidents to determine impact, cause and opportunities for corrective action. The amount of security incident data is currently statistically insignificantly small. Should the amount of data increase, Google will consider sharing this statistical information.
	XXIII. Searches	
PS-11.0	Establish a policy, as permitted by local laws, which allows security to randomly search persons, bags, packages, and personal items for client content. Implementation Guidance: • Communicate policies regarding search to all company personnel and third party workers • Consider conducting searches periodically of company personnel and third party workers to validate policy Note: Not all sites require a search policy. This should be determined based on risk per MS-2.1 and facility type.	See Row PS-9.1
PS-11.1	Implement an exit search process that is applicable to all facility personnel and visitors, including: • Removal of all outer coats, hats, and belts for inspection • Removal of all pocket contents • Performance of a self-pat-down with the supervision of security • Thorough inspection of all bags • Inspection of laptops' CD/DVD tray • Scanning of individuals with a handheld metal detector used within three inches of the individual searched Implementation Guidance:	See Row PS-9.1

	• Instruct security guards to look for items that are restricted from being brought onsite (e.g., cameras) or film materials which are not allowed to be brought offsite without proper authorization • Communicate policies regarding exit search to all company personnel and third party workers • Stagger shift changes to prevent long lines and extended wait times • This control is only applicable for facilities that perform CD/DVD or other physical device replication and where laws allow implementation	
PS-11.2	Prohibit personnel from entering/exiting the facility with digital recording devices (e.g., USB thumb drives, digital cameras, cell phones) and include the search of these devices as part of the exit search procedure. Implementation Guidance: • Confiscate any digital recording devices that are detected and store them in secured lockers • Document any incidents of attempted content theft • Take the necessary disciplinary action for individuals attempting content theft Implement and enforce a policy to prohibit mobile/cellular devices with digital recording capabilities • Allow cell phones with digital recording capabilities if tamper-evident stickers are used • If an exception has been documented and approved in writing by the client that permits use of digital devices in restricted areas, use of those devices when content is open and viewable is still prohibited	See Row PS-9.1
PS-11.3	Enforce the use of transparent plastic bags and food containers for any food brought into production areas. Implementation Guidance: • Consider designating an area for eating food outside of the production area	See Row PS-9.1
PS-11.4	Implement a dress code policy that prohibits the use of oversized clothing (e.g., baggy pants, oversized hooded sweatshirts).	See Row PS-9.1
PS-11.5	Use numbered tamper-evident stickers/holograms to identify authorized devices that can be taken in and out of the facility.	See Row PS-9.1
PS-11.6	Implement a process to test the exit search procedure. Implementation Guidance: • Perform periodic audits of the search process to ensure that security guards are thorough with their searches • Identify ways to improve the exit search process • Document all audits of and improvements to the search process	Google maintains and implements a robust and comprehensive internal and external audit plan that is performed at least annually to test the efficiency and effectiveness of implemented security controls. Google provides audits assertions using industry accepted formats such as ISAE 3402, SOC 2/3 and ISO/IEC 27001.
PS-11.7	Perform a random vehicle search process when exiting the facility parking lot.	See Row PS-9.1

PS-11.8	Segregate replication lines that process highly sensitive content and perform searches upon exiting segregated areas.	See Row PS-13.1 See Row PS-6.1
PS-11.9	Implement additional controls to monitor security guards activity. Implementation Guidance: • Review the exit search process for security guards upon exit • Segregate security guard responsibilities for overseeing plant/production areas from exit points (e.g., search process)	See Row PS-9.1
	XXIV. Inventory Tracking	
PS-12.0	Implement a content asset management system to provide detailed tracking of physical assets (i.e., received from client created at the facility). Implementation Guidance: • Require a release form or work order to confirm that content can be checked out by a specific individual • Require individuals to present identification for authentication • Require a tag (e.g., barcode, unique ID) for all assets • Log all assets that are checked-in/checked-out • Log the expected duration of each check out • Consider the use of an automated alert to provide notifications of assets that have not been returned by end of the business day, or the authorized period of time • Track and follow up with individuals that have outstanding checked-out assets • Log the location of each asset • Log the time and date of each transaction	Google maintains assets inventories and assigns ownership for managing its critical resources. Google tags physical hardware. Components are inventoried for easy identification and tracking within Google facilities. For production servers hosted in data centers, Google uses an internal system used by data center teams to track assets. Teams maintain asset inventories for the assets they are responsible for (e.g. data center, corporate hardware). Every asset at Google has an inventory tag - if it's not inventoried then it will be flagged during continuous monitoring. There is an automated system that is monitoring all data sources Google Cloud Compute resources support tagging. Customers assign tags to help easily apply networking or firewall settings. Tags are used by networks and firewalls to identify which instances that certain firewall rules apply to. For example, if there are several instances that perform the same task, such as serving a large website, you can tag these instances with a shared word or term and then use that tag to give HTTP access to those instances. Tags are also reflected in the metadata server, so you can use them for applications running on your instances. Refer here for more details. Google tags physical hardware. Components are inventoried for easy identification and tracking within Google facilities. Other hardware characteristics such as MAC are also used for identification. Google allows domain administrators to configure alerts for potential suspicious logins. Geographic location is one factor that could indicate a suspicious login. Customers can apply their own data-labeling standard to information stored in Google Cloud.
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 the vault when not in use. Implementation Guidance: • Apply dual barcodes to track assets (i.e., barcode on both the asset and the container/case) • Send assets directly to the vault after being barcoded and return assets to the vault immediately when no longer needed	See Row PS-12.0

PS-12.1.1	Develop a data classification scheme to categorize physical assets of differing security requirements. (Reordered and renumbered, previously PS-12.1.2) Implementation Guidance: ● Define security levels of content according to risk ● Ensure data classifications are consistent with client requirements ● Data classification schemes are particularly important in facilities that work on different types of content, e.g. catalog, TV, and theatrical in same environment	See Row PS-12.0
PS-12.2	Retain asset movement transaction logs for at least one year. Implementation Guidance: ● Store physical or digital logs for all asset movements; logs should include: ○ Barcode or unique ID of asset that was checked in/checked-out ○ Time and date of check-in/check-out ○ Name and unique ID of the individual who checked out an asset ○ Reason for checkout ○ Location of asset	See Row PS-9.1
PS-12.3	Review logs from the content asset management system at least weekly and investigate anomalies. Implementation Guidance: ● Identify assets that have not been returned by the expected return date ● Follow up with individuals who last checked out assets that are missing ● Implement disciplinary procedures for individuals who do not follow asset management policies ● Consider implementing automated notification when assets are checked out for extended periods of time	Google has implemented network and host based tools to detect and respond to potential security incidents. Google maintains automated log collection and analysis tools to support investigations. Google restricts physical and logical access to audit logs. Google has mapped its security controls to the requirements of SOC 2/3, NIST 800-53 Rev. 3 and ISO/IEC 27002. Google maintains an automated log collection and analysis tool to review and analyse log events.
PS-12.4	Use studio film title aliases on physical assets and in asset tracking systems. Implementation Guidance: ● Consider removing the studio name on physical assets, when appropriate	This doesn't apply to Google Cloud Operations.
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. Implementation Guidance: ● Perform daily aging reports either manually or through an asset management system ● Investigate all exceptions	See Row PS-9.1
PS-12.5.1	A documented process for checking out content should be established. Implementation Guidance: ● Guidelines should include, but are not limited to:	See Row PS-9.1

	○ Ensuring that checkout durations not exceed 24 hours or the duration of the custodian's shift unless explicitly approved in writing by management ○ Performing daily inventory checks to track content and investigate individuals who have not returned content in a timely manner ○ Using automatic system notifications to alert team members when content has not been returned within the expected timeframe	
PS-12.6	Lock up and log assets that are delayed or returned if shipments could not be delivered on time. Implementation Guidance: ● Establish a procedure for storing assets in an access controlled area ● Maintain documentation that logs the on-site storage of assets, including the date and reason for storage	See Row PS-9.1
	XXV. Inventory Counts	
PS-13.0	Perform a quarterly inventory count of each client's asset(s), reconcile against asset management records, and immediately communicate variances to clients.	Google maintains assets inventories and assigns ownership for managing its critical resources. Google maintains a list of subprocessors here. Refer here for more information on subprocessors.
PS-13.1	Segregate duties between the vault staff and individuals who are responsible for performing inventory counts. Implementation Guidance: ● Assign non-vault staff personnel to do random checks of count results	Google employs a vendor management process that includes contractual requirements to adhere to Google's security policies and onsite inspections, as needed, to confirm compliance. Google maintains a list of subprocessors. Refer here for more information on subprocessors, and Cloud Data Processing Addendum (subprocessor section).
	XXVI. Blank Media/ Raw Stock Tracking	
PS-14.0	Tag (e.g., barcode, assign unique identifier) blank stock/raw stock per unit when received. Implementation Guidance: ● Do not allow blank or raw media stock in secured production areas unless it is required for production purposes	See Row PS-13.1
PS-14.1	Establish a process to track consumption of raw materials (e.g., polycarbonate) monthly. Implementation Guidance: ● Reconcile existing raw stock with work orders to identify variances in inventory ● Establish a variance threshold that triggers the incident response process when exceeded ● Consider the execution of physical counts of raw stock as part of the monthly tracking process	See Row PS-13.1
PS-14.2	Store blank media/raw stock in a secured location. Implementation Guidance:	See Row PS-13.1

	• Require access controls (e.g., locked cabinet, safe) to prevent unauthorized access • Restrict access to blank media/raw stock to personnel responsible for output creation • Require individuals to present a proper work order request to check out blank media/raw stock	
	XXVII. Client Assets	
PS-15.0	Restrict access to finished client assets to personnel responsible for tracking and managing assets. Implementation Guidance: • Restrict access to only the vault staff, who can then authorize individuals to check out client assets when presented with a valid work order request • Segregate duties so that no member of the vault staff handles production data for processing	See Row PS-15.2 See Row PS-13.1
PS-15.1	Store client assets in a restricted and secure area (e.g., vault, safe, or other secure storage location). Implementation Guidance: • Implement an additional safe or high-security cage within the vault for highly sensitive titles • Sensitive content should also be stored in a secure segregated area (e.g., safe, cage or other isolated area) and segregated from other content • A safe weighing less than 300 lbs. should be secured to an immovable surface (e.g., floor, wall). Note: Bolting the safe may make its contents vulnerable to fire damage. This is not recommended for storing backups	See Row PS-9.1
PS-15.2	Consider requiring two company personnel with separate access cards or keys / pins to unlock highly sensitive areas (e.g., safe, high-security cage) after-hours.	Google maintains an automated access revocation process that includes account locking and revocation of certificates and role assignment. Google logs all changes in user permissions with the date and time of such changes.
PS-15.3	Use a locked fireproof safe to store undelivered packages that are kept at the facility overnight.	See Row PS-9.1
PS-15.4	Implement a dedicated, secure area (e.g., security cage, secure room) for the storage of undelivered screeners that are locked, access-controlled, and monitored with surveillance cameras and/or security guards. Implementation Guidance: • Limit access to personnel who require access for their job role • Ensure that the screener storage area is completely enclosed, locked and monitored at all times • Implement a process to review surveillance footage on a regular basis	Google Cloud customers may select specific regions to place data, based on product availability. Customers can choose data location when they initiate a project set up. This is covered by our service specific terms.
	XXVIII. Disposals	

PS-16.0	Require that rejected, damaged, and obsolete stock (DVDs, tapes, and other storage media) containing client assets be erased, degaussed, shredded, or physically destroyed before disposal. Implementation Guidance: • Implement processes to inventory and reconcile stock, and then securely recycle or destroy rejected, damaged, and obsolete stock • Irreparably damage media before placing into scrap bin • Consider referencing U.S. Department of Defense 5220.22-M for digital shredding and wiping standards	Google has strict policies and procedures to govern the management of the equipment lifecycle within its production data centers. Any disk that did, at any point in its lifecycle, contain customer data is subject to a series of data destruction processes before leaving Google's premises, and would need to be authorized by an appropriate operations manager before release. Refer here for more information.
PS-16.0.1	Finished elements (e.g., check discs, test prints, mockups, ADR scripts) should be destroyed immediately after use, unless otherwise specified by content owners. Require paper materials containing client assets (scripts, artwork, storyboards, etc.) be physically destroyed before disposal. Implementation Guidance: • Shredders must cut paper in a cross-hatch pattern • Shred bins must be locked with openings small enough that a hand cannot fit inside • Restrict keys to shred bins on a least privilege basis • Purge Copier hard drives on at least a weekly basis	See Row PS-16.0
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. Implementation Guidance: • Establish and implement policies that limit the duration (e.g., 30 days) of storing rejected, damaged, and obsolete stock before recycling/destruction • Keep highly sensitive assets in secure areas (e.g., vault, safe) prior to recycling/destruction • Ensure that disposal bins are locked	See Row PS-15.4
PS-16.2	Maintain a log of asset disposal for at least 12 months. Implementation Guidance: • Integrate the logging of asset disposal into the asset management process • Include a final disposal record for disposed assets in disposal logs	See Row PS-16.0
PS-16.3	Destruction must be performed on site. On site destruction must be supervised and signed off by two company personnel. If a third party destruction company is engaged, destruction must be supervised and signed off by two company personnel and certificates of destruction must be retained. Implementation Guidance: • Consider requiring the following information on the certificate of destruction:	See Row PS-16.0

	○ Date of destruction ○ Description of the asset destroyed/disposed of Method of destruction ○ Name of individual who destroyed the assets	
PS-16.4	Use automation to transfer rejected discs from replication machines directly into scrap bins (no machine operator handling). Implementation Guidance: ● Use segregation of duties (e.g., personnel who create the check disc are separate from personnel who destroy the disc) where automated disposal is not an option ● Maintain a signed log of the date and time when the disc was disposed	Google provides (under a specific NDA) customers with a SOC 2/3 report that includes testing of Google's access controls. For further details on Google Cloud's access controls, refer to this security whitepaper.
	XXIX. Shipping	
PS-17.0	Require the facility to generate a valid work/shipping order to authorize client asset shipments out of the facility. Implementation Guidance: ● Include the following information on the work/shipping order: ○ Work/shipping order number ○ Name and company of individual who will pick up content ○ Time and date of pick up ○ Facility contact ● Create a form for documenting outbound assets that are transported via uncommon methods	See Row PS-13.1 Google provides customers with security documentation including a security whitepaper and SOC 2/3 report that describe how we operate a global network with replication, failover and offsite backups. For Google Cloud users, the locality of data is for the most part customer controlled and is described here.
PS-17.1	Track and log client asset shipping details; at a minimum, include the following: ● Time of shipment ● Sender name and signature ● Recipient name ● Address of destination ● Tracking number from courier ● Reference to the corresponding work order Implementation Guidance: ● Require recipient signature ● Retain shipping logs for a minimum of 1 year	See Row PS-13.1
PS-17.2	Secure client assets that are waiting to be picked up. Implementation Guidance: ● Lock all doors and windows to shipping and receiving areas when unattended ● Assets must be locked up until handed off to the vendor/courier ● Camera surveillance should be used to monitor content that is being staged prior to shipping. If appropriate, it should also be used to capture the transfer of a package from the facility to the courier.	See Row PS-13.1

	• Drives, reels, DVDs to be shipped should be brought to the public loading area only after the truck arrives.	
PS-17.3	Validate client assets leaving the facility against a valid work/shipping order. Implementation Guidance: • Request valid identification from couriers and delivery personnel to authenticate individuals picking up shipments against the corresponding work order • Confirm that the shipped count matches the shipping documentation • Report back any discrepancies or damage to shipped goods immediately	See Row PS-13.1
PS-17.4	Prohibit couriers and delivery personnel from entering content / production areas of the facility. Implementation Guidance: • Escort delivery personnel if access to content / production areas is necessary	See Row PS-13.1 See Row PS-4.0

PS-17.5	Document and retain a separate log for truck driver information.
	
	Implementation Guidance:
	• Maintain a log of all truck drivers and include the following information:
	  ○ Name
	  ○ License tags for the tractor and trailer
	  ○ Affiliated company
	  ○ Time and date of pick up
	  ○ Content handled
		See Row PS-13.1

PS-17.5.1	Facilities should implement and maintain a record of all delivery personnel entering and exiting the building.	.See Row PS-13.1
PS-17.6	Observe and monitor the on-site packing and sealing of trailers prior to shipping. Implementation Guidance: • Require security personnel to be present at all times while trailers are loaded and sealed	See Row PS-13.1
PS-17.7	Record, monitor and review travel times, routes, and delivery times for shipments between facilities. Implementation Guidance: • Establish a baseline for delivery times between common shipping points and monitor actual times for variance • Investigate, report, and escalate major variances to appropriate personnel • Designate approved rest stops • Consider implementing a real-time GPS tracking system to monitor and alert on unexpected delays	This doesn't apply to Google Cloud operations
PS-17.8	Prohibit the transfer of film elements outside of the shipping department unless approved by the client.	This doesn't apply to Google Cloud Operations.

	Implementation Guidance: ● Treat film elements like any other piece of physical media, using the same controls for shipping and receiving.	
PS-17.9	Ship prints for pre-theatrical screenings in segments (e.g., odd versus even reels).	This doesn't apply to Google Cloud Operations.
	XXX. Receiving	
PS-18.0	Inspect delivered client assets upon receipt and compare to shipping documents (e.g., packing slip, manifest log). Implementation Guidance: ● Identify and log any discrepancies (e.g., missing items, damaged media) ● Report discrepancies to management, clients, and/or the sender immediately	See Row PS-13.1
PS-18.1	Maintain a receiving log to be filled out by designated personnel upon receipt of deliveries. Implementation Guidance: ● Record the following information: ○ Name and signature of courier/delivering entity ○ Name and signature of recipient ○ Time and date of receipt ○ Details of received asset	See Row PS-13.1
PS-18.2	Perform the following actions immediately: ● Tag (e.g., barcode, assign unique identifier) received assets ● Input the asset into the asset management system ● Move the asset to the restricted area (e.g., vault, safe) Implementation Guidance: ● Store received assets that cannot be immediately tagged and vaulted in a secure staging area (e.g., high-security cage)	See Row PS-13.0
PS-18.3	Implement a secure method for receiving overnight deliveries. Implementation Guidance: ● Ensure that schedules for expected items are only available to people who need to see them	Where applicable overnight deliveries will be secured.
	XXXI. Labeling	
PS-19.0	Prohibit the use of title information, including AKAs ("aliases"), on the outside of packages unless instructed otherwise by client.	Google maintains policies and procedures on data access and labeling. Customers can apply their own data-labeling standard to information stored in Google Cloud. Customers may leverage Google's AI Platform Data Labeling Service to do so.
	XXXII. Packaging	

PS-20.0	Ship all client assets in closed/sealed containers, and use locked containers depending on asset value, or if instructed by the client.	This does not apply to Google Cloud operations.
PS-20.1	Implement at least one of the following controls: • Tamper-evident tape • Tamper-evident packaging • Tamper-evident seals (e.g., in the form of holograms) • Secure containers (e.g., Pelican case with a combination lock) Implementation Guidance: • Establish and communicate a plan for how to handle goods that have been tampered with • Report all instances of tampering to the Incident Response Team (MS-5.0)	This does not apply to Google Cloud operations.
PS-20.2	Apply shrink wrapping to all shipments, and inspect packaging before final shipment to ensure that it is adequately wrapped. Implementation Guidance: • Apply shrink wrapping to individual assets (e.g., skids, pallets) or per spindle if bulk shipments are performed	This does not apply to Google Cloud Operations.
	XXXIII. Transport Vehicles	
PS-21.0	Lock automobiles and trucks at all times, and do not place packages in clear view. Implementation Guidance: • Do not leave packages unattended	See Row PS-13.1
PS-21.1	Include the following security features in transportation vehicles (e.g., trailers): • Segregation from driver cabin • Ability to lock and seal cargo area doors • GPS for high-security shipments Implementation Guidance: • Use vehicles equipped with GPS tracking systems for delivery of sensitive content and high-value assets	Google maintains assets inventories and assigns ownership for managing its critical resources. See Row PS-13.1
PS-21.2	Apply numbered seals on cargo doors for shipments of highly sensitive titles. Implementation Guidance: • Require security guards to apply, record, and monitor seals • Consider additional security measures for highly sensitive packages (e.g., locked/secured cargo area, locked pelican cases	This does not apply to Google Cloud Operations.
PS-21.3	Require security escorts to be used when delivering highly sensitive content to high-risk areas. Implementation Guidance:	This does not apply to Google Cloud Operations.

	• Hire security personnel capable of protecting highly sensitive content from hijacking, mugging, and other scenarios that could result in content theft	
	XXXIV. Environmental	

PS-22.0	Maintain optimal temperature and humidity set-points to facilitate optimal performance of equipment and to reduce the likelihood of catastrophic hardware failures for areas that house servers, storage devices, LAN equipment, network communications devices, and storage media.
	
	Implementation Guidance:
	• Recommended temperature and humidity settings:
	  ○ Temperature (Low End): 64.4 F (18 C)
	  ○ Temperature (High End): 80.6 (27 C)
	  ○ Moisture (Low End): 40% relative humidity and 41.9 F (5.5 C) dew point
	  ○ Moisture (High End): 60% relative humidity and 59 F (15 C) dew point
		Google adheres to ISO/IEC 27001/17/18, SOC 1/2/3, PCI DSS, and several other global and regional standards and frameworks, for securing,monitoring, maintaining and testing of datacenter utilities services and environmental conditions.
		
		Google reduces the environmental impact of running our data centers by designing and building our own facilities. We install smart temperature controls, use "free-cooling" techniques like using outside air or reused water for cooling, and redesign how power is distributed to reduce unnecessary energy loss.
		
		To gauge improvements, we calculate the performance of each facility using comprehensive efficiency measurements. We're the first major Internet services company to gain external certification of our high environmental, workplace safety and energy management standards throughout our data centers. Specifically, we received voluntary ISO/IEC 50001 certification and incorporated our own protocols to go beyond standards.
		
		Refer to the Google Security White Paper for further details.

	XXXV. External Network/WAN	

DS-1.0	Separate external network(s)/WAN(s) from the internal network(s) by using inspection firewall(s) with Access Control Lists that prevent unauthorized access to any internal network and with the ability to keep up with upload and download traffic.
	
	Implementation Guidance:
	• Remote and WFH locations must have a firewall to segregate the WAN (Internet) from the internal network used to access content
	• Configure WAN firewalls with Access Control Lists that deny all traffic to any internal network other than to explicit hosts that reside on the DMZ
	• Configure the WAN network to prohibit direct network access to the internal content / production network
	• Include detailed WAN documentation that accurately shows and describes the number of connections to and from all external facing devices
	• Firewall rules must be configured to generate logs for all traffic and for all configuration changes, and logs should be inspected on at least a monthly basis
	• Firewall should have a subscription to anti-virus and intrusion detection updates, and updates should occur at least once per week
	• Consider including the following in the firewall configuration:
	  ○ Anti-spoofing filters
	  ○ Block non-routable IP addresses
	  ○ Block internal addresses over external ports
	  ○ Block UDP and ICMP echo requests
	  ○ Block unused ports and services
	  ○ Block unauthorized DNS zone transfers
	• Apply egress filtering, so outgoing traffic can only come from an internal address
		See Row DS-3.7
		
		See Row PS-6.1

DS-1.1	Implement a process to review firewall Access Control Lists (ACLs) to confirm configuration settings are appropriate and required by the business every 6 months. Implementation Guidance: • Export ACLs from firewalls and/or routers • Review ACLs to confirm that network access is appropriate • Require management sign-off of review, as well as any firewall rule changes Records of all externally accessible servers as well as each business case and system owner of each server should be maintained • Update ACLs accordingly	Google maintains these diagrams for internal purposes, but due the dynamic and sensitive nature of the information, does not share it externally. The security state of network devices is monitored continuously. Network ACLs are documented within configuration files with comments on purpose, as appropriate. Google provides solution papers and reference docs for various architectures and intended solutions.
DS-1.2	Deny all incoming and outgoing network requests by default. Enable only explicitly defined incoming requests by specific protocol and destination. Enable only explicitly defined outgoing requests by specific protocol and source. Implementation Guidance: • Block all unused ports and services • For externally accessible hosts, only allow incoming requests to needed ports on those hosts • Restrict all unencrypted communication protocols such as Telnet and FTP • Replace unencrypted protocols with encrypted versions	Google builds its own machines and deploys custom operating system images that only permit the necessary ports, protocols and services.
DS-1.2.1	Firewalls should be configured to actively alert security members of key security events Implementation Guidance: It is suggested to implement the following: At a minimum: • Security events tagged for audit should generate an alert to be sent to the firewall administrator or Information Security team • The firewall administrator should review the alert in a timely manner based on the severity of the incident as documented in the Security or Incident Response policy • Findings from all investigations should be documented • Corrective actions should be taken to prevent malicious traffic	Google has mechanisms in which all Google managed Mac, Windows, and Linux computers have personal firewalls enabled and managed by an internal team. For CrOS devices, the functionality offered by personal firewalls is already built in. Google maintains a security monitoring program to detect and report security related events in our infrastructure and applications. Google discusses monitoring in the security whitepaper: https://cloud.google.com/security/overview/whitepaper Google uses a proprietary event management tool to identify and alert on unauthorized use of the information system and assets and takes timely appropriate action when unauthorized use is detected.
DS-1.3	Place externally accessible servers (e.g., web servers, remote access servers (e.g., VPN gateways, remote access brokers, etc.) within a DMZ VLAN or a public subnet DMZ within a VPC (Virtual Private Cloud) and not on an internal network.. Implementation Guidance: • Isolate servers in the DMZ to provide only one type of service per server (e.g., web server, etc.) • Implement ACLs to restrict access to the internal network from the DMZ, or access from public subnets to private subnets within a VPC.	In Google's production environment, traffic is required to flow through defined proxies in order to connect to the external environment. The defined proxies are spread across internal services managed by Google's Traffic team. They have RPC policy limitations enforced and they are limited at the network edge ACLs to permit return of traffic to specific sets of ports and protocols. Google has a security whitepaper which discusses defense in depth: https://cloud.google.com/security/overview/whitepaper

DS-1.4	Implement a process to patch network infrastructure devices (e.g., firewalls, routers, switches, etc.), SAN/NAS (Storage Area Networks and Network Attached Storage), and servers. Implementation Guidance: • Implement a regular (e.g. monthly) process to identify, evaluate and test patches for network infrastructure devices, SAN/NAS and servers • Update network infrastructure devices, SAN/NAS, and servers to patch levels that address significant security vulnerabilities • Address critical patches within 48 hours • Consider the deployment of a centrally managed patch management system • Implement virtual patches using the IDS/IPS, for zero-day vulnerabilities, where patches are unavailable and until a software patch is available	Google has a dedicated process tied to the SLDC for patching all network devices and equipment.
DS-1.5	Harden network infrastructure devices, SAN/NAS, and servers based on security configuration standards. Disable SNMP (Simple Network Management Protocol) if it is not in use or use only SNMPv3 or higher and select SNMP community strings that are strong passwords. Implementation Guidance: • This also applies to equipment used by WFH /remote workers when content is stored locally on the endpoint, for devices such as a NAS, WIFI router, and firewall used for networking Consider the following hardening options: ○ Disable guest accounts and shares Install anti-virus / anti-malware ○ Enable software firewalls ○ Remove unnecessary software Uninstall/disable unneeded services ○ Require all users to run as restricted users ○ Use an ACL that restricts access to the device so that only authorized management systems may be used to connect using SNMP ○ Refer to the following security hardening standards for hardening network infrastructure devices: ■ NIST ■ SANS ■ NSA	See Row DS-1.2
DS-1.6	Do not allow direct management of the firewall from any external interfaces (i.e. Internet or WAN facing). Implementation Guidance: • For corporate administration and maintenance functions not conducted on the internal network use multi-factor (MFA) authentication and a VPN connection with advanced encryption standard (AES-256) to carry out remote administration functions	All access to production systems are based on least privilege, requires two-factor authentication, and is logged.

DS-1.7	Store local backups of network infrastructure / SAN/NAS devices and servers on a server in a secure internal network. Implementation Guidance: • Configure network infrastructure devices to store backups of configuration files in a secure manner (e.g., encrypted) on the internal network • Ensure that only authorized administrators have access to the storage location and the encrypted backups • Ensure that restrictions are in place to mitigate brute-force attacks and unauthorized access to the configuration files if Trivial File • Transfer Protocol (TFTP) is used for backups	See Row MS-6.2
DS-1.8	Perform on at least a monthly basis network vulnerability scans of all external IP ranges and hosts and remediate issues. Implementation Guidance: • Native cloud assessment tools may also be leveraged in lieu of cloud vulnerability scans (e.g., Inspector, Config, Guard Duty, and Trusted Advisor) • Remediate critical issues that could allow unauthorized access to content within 48 hours. • Remediate non critical issues in a timely manner • Ensure that tools used for scanning/testing accommodate virtualization technologies, if being used • Consider having this performed by an independent third party • Consider both authenticated and unauthenticated scans for improved vulnerability detection	See Row PS-5.6
DS-1.9	Perform on at least an annual basis, penetration testing of all external IP ranges and hosts and remediate issues. Implementation Guidance: • Remediate critical issues that could allow unauthorized access to content within 48 hours. • Remediate non critical issues in a timely manner • Ensure that tools used for scanning/testing accommodate virtualization technologies, if being used • Consider having this performed by an independent third party.	See Row PS-5.6
DS-1.10	Secure any point to point connections by using dedicated, private connections and / or encryption. Implementation Guidance: • Connections over the Internet or public networks should be encrypted using site-to-site VPN • Consider encrypting connections over private connections (e.g. dark fiber, leased lines, frame relay, MPLS, etc.)	See Row DS-9.01 See Row DS-11.1

	• Use advanced encryption standard (AES256) or higher for encryption • All point-to-point (e.g., VPN, private fiber, etc...) connections within the organization through which content travels should be documented and reviewed for usage and business validity at least every six months, three months recommended	
DS-1.11	Implement a synchronized time service protocol (e.g., Network Time Protocol) to ensure all systems have a common time reference. Implementation Guidance: • Ensure systems have the correct and consistent time • Ensure time data is protected • Ensure time settings are received from industry-accepted time sources	Google uses a synchronized time-service protocol to ensure all systems have a common time reference.
DS-1.12	Establish, document and implement baseline security requirements for WAN network infrastructure devices and services. Implementation Guidance: • Ensure system defaults that could create vulnerabilities are modified before being placed into production • Consider continuous monitoring to report compliance of infrastructure against security baselines	Google provides high-level information on our tools and techniques in our SOC report and security whitepaper. Google performs quality reviews on its code as part of our standard continuous build and release process. Google performs at least annual reviews of our data centers to ensure our physical infrastructure operating procedures are implemented and followed. For customer deployments, our resellers/integration partners take the lead on ensuring that the deployment meets the customer requirements. Our deployment teams provide technical support to troubleshoot issues. Google maintains a dashboard with service availability and service issues here: • https://status.cloud.google.com/ • https://www.google.com/appsstatus Google maintains internal bug tracking of known product defects. Each bug is assigned a priority and severity rating based on the number of customers impacted and the level of potential exposure of customer data. Bugs are actioned based on those ratings and remediation actions are captured in the bug tickets. If a legitimate vulnerability requiring remediation has been identified by Google, it is logged, prioritized according to severity, and assigned an owner. Google tracks such issues and follows up frequently until they can verify that they have been remediated. We also have a Vulnerability Rewards Program to solicit external reports in problems in our services here . Google follows a structured code development and release process. As part of this process, all code is peer reviewed. Google makes proprietary code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats. See Row DS-6.9

	XXXVI. Internet	
DS-2.0	Prohibit production network and all systems that process or store digital content from directly accessing the internet, including email. If a business case requires internet access from the production network or from systems that process or store digital content, only approved methods are allowed via use of a remote hosted application / desktop session. Implementation Guidance: ● Remote and WFH workers that access production networks should do so via a VDI (virtual desktop infrastructure) and/or a studio approved remote pixel streaming connection (e.g., PCoIP, RGS, Parsec, NICE DCV, etc.). ● The connection must be encrypted with a minimum of AES256. MFA authentication must be used to initiate the connection. Access should never be granted directly to the production network or machine and should be via an intermediary access broker. Ability to copy content locally, and mount drives must be locked down. ● Implement firewall rules to deny all outbound traffic by default and explicitly allow specific systems and ports that require outbound transmission to designated internal networks, such as anti-virus definition servers, patching servers, licensing servers (only when local licenses are not available), etc. ● Proxy license servers hosted on production networks are allowed provided that outgoing requests to the Internet are via non-persistent connections (open during a maintenance window) via strict ACLs. Patches directly to production workstations are allowed the same way (open during a maintenance window). ● Handle exceptions using an Internet gateway system (e.g., Citrix, Terminal Services, VNC, etc.) with the following controls: ○ The system is tightly controlled where web browsing is the only function of the server ○ Access to restricted sites is prohibited, including web based email sites, peer-to-peer, digital lockers, and other known malicious sites ○ Restrict content from being transferred to or from the system ○ Patch and update the system regularly with the latest virus definitions ○ Review system activity regularly ○ Block the mapping of local drives, block USB mass storage, block mapping of printers, block copy and paste functions, and block the download/upload to the Internet gateway system from the production network ● A KVM, A keyboard / video / mouse (KVM) solution to a machine with Internet access not connected to the production network, may also be considered Ensure that any physical ports on the KVM switch which are not in use are properly locked down.	See Row PS-6.1

DS-2.1	Implement - corporate filtering software or appliances that block the following: • Potential phishing emails • Prohibited file attachments (e.g., Visual Basic scripts, executables, etc.) • File size restrictions limited to 30 MB • Known domains that are sources of malware or viruses Implementation Guidance: • Corporate email filtering should also cover remote/WFH users and should also be considered for BYOD devices. • Identify restricted content types for email attachments and email message body • Implement an email filtering solution and configure based on restricted content types	See Row PS-6.1
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 for all corporate devices, regardless of location, and including remote/WFH locations. Implementation Guidance: • Implement web-filtering/proxy server software to detect and prevent access to malicious websites. • Use DNS filtering services on all enterprise assets to block access to known malicious domains.	See Row PS-16.4
	XXXVII. LAN/Internal Network	
DS-3.0	Isolate the content / production network from nonproduction networks (e.g., office network, DMZ, the internet etc.) by means of physical or logical network segmentation. Implementation Guidance: • Remote and WFH workers should implement this via firewall rules to isolate their production network from other networks, or by keeping their production machine physically 'air gapped' without connections to the internet and other networks. The production network may also be separated via a studio approved remote pixel streaming connection (e.g., PCoIP, RGS, Parsec, NICE DCV, etc.) and access broker, if the production network is hosted separately from the location of the remote worker. They should not be able to copy the content to their local machine, or mount drives via the remote connection • Define Access Control Lists that explicitly allow access to the content / production network from specific hosts that require access (e.g., anti-virus server, patch management server, content delivery server, etc.) • Include explicitly defined ports and services that should allow access in the Access Control Lists • Segment or segregate networks based on defined security zones • Production (content) networks should be segmented from non-production networks	See Row PS-6.1

	• Corporate, WIFI, DMZ, Services (e.g., printers, cameras, servers), I/O, etc.) via the following methods:
	  ○ Physical Air Gap
	  ○ Logical segmentation via Layer 2 VLAN
	  ○ Logical segmentation via Layer 3 VLAN
	• Implement firewall rules to deny all outbound traffic by default and explicitly allow specific systems and ports that require outbound transmission to designated internal networks, such as anti-virus definition servers, patching servers, content delivery servers, licensing servers (only when local licensing servers are not available), etc.
	• Implement firewall rules to deny all inbound traffic by default and explicitly allow specific systems and ports that require inbound transmission from designated content delivery servers.
	• Refer to DS-2.0 for guidance on accessing the Internet on the production environment
	• Assign static IP addresses by MAC address on switches
	• Disable DHCP on the content / production network
	• Prohibit any production computer system from connecting to more than one network at a time
	• Prohibit content from being used or stored in nonproduction networks	

DS-3.1	Restrict access to the content / production systems to authorized computing hardware. Implementation Guidance: • Consider using physical Ethernet cable locks to ensure that a network cable cannot be connected to an alternate/unauthorized device	See Row DS-1.6
DS-3.2	Remote access into company networks should be restricted following a tiered approach, depending on the level of access required, and whether or not access will be to a content/production network. Access tiers will fall into the following general tiers: Tier 1: Access only to a corporate network or service that doesn't store content (e.g., VPN to corporate VLAN for file share access, Webmail, Office365, etc.) Tier 2: Remote worker (WFH) access to a content production network via studio approved pixel streaming (e.g., PCoIP, RGS, Parsec, NICE DCV, etc.) to perform post-production, VFX work etc. Tier 3: Restricted VPN administrative access to a production network, to perform maintenance work or approved personnel requiring elevated access to perform their job responsibilities. Implementation Guidance: • All tiers of remote access require MFA authentication • All tiers of access require an encrypted connection using AES 256 encryption	See Row PS-15.2

	• Tier 1 is for the general office worker, who does not require access to a production network for work or administrative purposes. • Tier 2, must not allow any access to copy content files to the local machine • Tier 2 access to a production network should only be granted via an access broker that is on a non-production network (e.g., DMZ) • Tier 3 must be a VPN connection to a launchpad/bastion host as an intermediate machine ('jump box') from a non-production network, to connect to the production network, without any direct connection to production allowed from the internet • Remote access accounts should not be shared (use individual, unique accounts) • The remote access user account list should be reviewed quarterly at a minimum. Accounts that are no longer active should be disabled • Upon termination, an employee remote access should be immediately disabled • Maintain a list of company personnel who are allowed remote access to the content / production network • Avoid use of the following methods for remote access: FTP, Telnet, SSH, IRC, IM • Remote access should be logged real time with alerts generated to administrators for suspicious activity and reviewed. • Administrators should have access to revoke remote access immediately, if remote access appears to have been compromised • VPN configuration must not allow split tunneling	
DS-3.3	Use switches/layer 3 devices to manage network traffic. Disable all unused switch ports on the content / production network to prevent access from unauthorized devices. Implementation Guidance: • Port security should be enabled • Use an secure protocol for accessing management interfaces • Use device administrator credentials with strong passwords • Separate password for exec commands if supported by the device • Disable unused ports on switches • Implement MAC filtering • Implement network based access control, i.e. 802.1X • Enable logging • If layer 2 switches are still in use, ensure that a firewall, router, or other higher layer network communications device is providing network isolation / traffic control.	See Row DS-1.1 See Row DS-1.2
DS-3.4	Restrict the use of non-switched devices such as hubs and repeaters on the content/production network (Re added) Implementation Guidance: • Replace all hubs/repeats with switches or layer 3 devices (Re added)	See Row DS-1.1 Google maintains one homogeneous operating environment for Google Cloud. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google intrusion detection involves: 1. Tightly controlling the size and make-up of Google's attack surface through preventative measures;

		2. Employing intelligent detection controls at data entry points; and 3. Employing technologies that automatically remedy certain dangerous situations.
DS-3.5	Prohibit bridging or dual-homed networking (physical network bridging) on computer systems between content / production networks and non-content / production networks. Implementation Guidance: ● Production workstations should not contain multiple NIC cards unless deemed necessary (e.g., metadata, video/audio sync). ● If multiple NIC cards are in use, connections must span between secure networks (i.e., spanning across both nonsecure and secure networks is prohibited). ● The server blade chassis should not have hot-swapping ability enabled for network interfaces (e.g., HPVPLEX or Cisco B22) ● Server blade systems should not have physical connectivity to the Data I/O networks and production networks at the same time. ● Different network or storage interfaces should not be provisioned to the same blade chassis ● Systems should not have connectivity to the data I/O networks and content / production networks at the same time. ● Systems that require connectivity to a like production and a metadata network (i.e. Stornext) are exempt from the bridging exclusion.	See Row DS-1.1 See Row DS-3.4
DS-3.6	Implement a network-based intrusion detection /prevention system (IDS / IPS) to protect the content / production network. Other Basic Border Gateway services (e.g., Gateway AntiVirus, and URL Filtering) should also be enabled. Implementation Guidance: ● Configure the network-based intrusion detection / prevention system (IDS / IPS) to alert on / prevent suspicious network activity ● The IDS / IPS administrator should review those events immediately and document findings from all investigations. ● Subscribe to anti-virus/anti-malware for the IDS / IPS Update attack signature definitions/policies and antivirus/anti-malware on the IDS / IPS on at least a weekly basis ● Update attack signature definitions/policies and anti-virus/antimalware on the IDS / IPS on at least a weekly basis ● Log all activity and configuration changes for the IDS / IPS ● Considering implementing host-based intrusion detection system software on all workstations ● Enable virtual patching in the IDS/IPS, where software patches may be unavailable for applications and devices	See Row DS-3.7 See Row DS-3.4
DS-3.7	Disable SNMP (Simple Network Management Protocol) if it is not in use. Use SNMPv3 or higher with strong passwords for community strings	Google does not permit wireless access in the production environment. Google has established policies and procedures to manage its corporate wireless network perimeter. Google does not permit wireless access points in its production environment and periodically scans for rogue devices. Google has established strong encryption and authentication to its corporate wireless network.

	Implementation Guidance: • Use an ACL that restricts access to the SNMP device so that only authorized management systems from trusted zones may be used to connect. • Community strings must be different from those used in login credentials of security administration accounts.	
DS-3.8	Harden systems prior to placing them in the LAN / Internal Network. Implementation Guidance: • Refer to DS-1.5 for suggestions	See Row DS-1.2

DS-3.9	Conduct internal network vulnerability scans and remediate any issues, at least annually
	
	Implementation Guidance:
	• Remote and WFH workers that handle content on their local corporate endpoint machine should have their equipment and devices scanned at least quarterly.
	• Remote and WFH workers that connect to content production networks via a studio approved remote pixel streaming connection (e.g., PCoIP, RGS, Parsec, NICE DCV, etc.), should have their equipment and devices on the production network where the content is stored, scanned at least quarterly
	• Ensure that tools used for scanning accommodate virtualization technologies, if being used
	• Consider using authenticated scans. Include the following:
	  ○ Production networks
	  ○ Non-Production networks
	  ○ Connected machines / devices
	  ○ Non-connected machines / devices
		See Row PS-5.6

DS-3.10	Store local backups of local area network, SAN/NAS, devices, servers and workstations on a server in a secure internal network. Implementation Guidance: • Configure local area network devices to store backups of configuration files in a secure manner (e.g., encrypted using AES 256) on a secure internal network • Ensure that only authorized administrators have access to the storage location and the encrypted backups	See Row MS-6.2

DS-3.11	Domain Name System (DNS) Servers should be securely configured, and only trusted DNS Servers should be used for domain name resolution.
	
	Implementation Guidance:
	• DNS Server should be on non-production networks
	• Harden DNS servers prior to deployment to include the following items:
	  ○ Regular patching and updates as per DS-6.4, including software, and operating systems
	  ○ Removing unnecessary software
	  ○ DNS version hiding
		See Row DS-6.1

	○ Administration access should be performed through MFA ○ Restricting administrative privileges to authorized individuals ● To prevent DNS cache poisoning disable recursive queries, enable iterative queries, and implement DNSSEC ● Consider DNS over TLS (DOT) or DNS over HTTPS (DOH) ● Restrict zone transfers to trusted IP addresses ● Consider implementing TSIG ● Enable DNS audit logging ● Periodic reviews of DNS audit logs ● Periodic reviews of DNS zones	
	XXXVIII. Wireless	
DS-4.0	Prohibit wireless networking and the use of wireless devices on the content / production network. <u>Implementation Guidance:</u> ● WFH and Remote worker machines and production networks must not be connected to a wireless network while accessing content locally. ● Restrict wireless guest networks to access only the Internet and not the content / production network ● Wireless network access cards (NICs) should be disconnected from production computers either physically, or via endpoint security policy (e.g. Active Directory Group Policy Object, etc.)	See Row PS-6.1 See Row DS-3.7
DS-4.1	Configure non-production wireless networks (e.g., administrative and guest) with the following security controls: ● Disable WEP / WPA Enable WPA2-PSK (AES) ● Segregate “guest” networks from the company’s other networks ● Change default administrator logon credentials ● Change default network name (SSID) <u>Implementation Guidance:</u> ● Consider additional security controls such as: ○ Use non-company, non-production, specific SSID names ○ RADIUS for authentication where the option is available WPA2-Enterprise (AES) if applicable ○ MAC address filtering ○ Blacklist the wireless MAC addresses of production workstations and devices ○ Configure the wireless access point / controller to broadcast only within the required range ○ Consider implementing port based network access control (e.g. 802.1X framework for wireless networking) which includes the following: ■ Remote Access Dial In User Service (RADIUS) for Authentication, Authorization and Accounting	See Row DS-11.1 See Row DS-3.7

	■ Lightweight Directory Access Protocol (LDAP) server, such as Active Directory, to manage user accounts ■ Public Key Infrastructure to generate and manage client and server certificates ○ Implement the following controls if pre-shared keys must be used: ■ Configure WPA2 with CCMP (AES) ■ Set a complex passphrase (See DS-8.1 for passphrase complexity recommendations) ■ Change the passphrase at least every 90 days and when key company personnel terminate their employment	
DS-4.2	Implement a process to scan for rogue wireless access points and remediate any validated issues. Implementation Guidance: ● Implement a process to roam and scan the facility for unprotected wireless access points at least quarterly ● Configure a centralized wireless access solution (i.e., wireless controller) to alert administrators of rogue wireless access points upon detection, if possible	See Row DS-3.7
	XXXIX. I/O Device Security	
DS-5.0	Designate specific data I/O systems to be used for uploading / downloading content from / to external networks (Internet). Implementation Guidance: ● WFH and Remote workers that ingest content using their machine, should always be disconnected from internet after content download, during production work, and after content upload. ● If content is not downloaded or uploaded by WFH and remote workers and is only accessed via a studio approved remote pixel streaming connection (e.g., PCoIP, RGS, Parsec, NICE DCV, etc.) then the previous point is not applicable. ● Implement ACLs to allow traffic between the content / production network and systems used for I/O for specific source/destination IP addresses ● Implement whitelisting to restrict content downloads and uploads to only authorized external sources and destinations ● If FQDN (Fully Qualified Domain Names) are used, the firewall should contain a valid DNS entry. DNS resolution should be confirmed it is refreshing periodically to ensure the latest IP addresses are captured in the ACL. ● Implement allow listing to restrict content downloads and uploads to only authorized external sources and destinations	IO paths in all data centers are tightly controlled and monitored.

DS-5.0.1	Implement a multi-layered network architecture for ingesting content from external networks (Internet) into the production network, and moving content from the production network to external networks. Implementation Guidance: ● Implement separate isolated networks for data I/O and production. ● Use dedicated data I/O workstations to move content between external networks (Internet) and inbox / outbox storage. ● Inbox / outbox storage should be local to data I/O workstations or located in data I/O network ● Use a separate set of credentials, one for the data I/O side, and another for the production side to access the inbox/outbox storage ● Data movement must be initiated from the more secure layer: i.e. push / pull content at the data I/O zone to / from Internet; push / pull content at the production network to / from the data IO zone ● Accordingly, implement strict (IP and port) layer 2/3 ACLs to allow outbound network requests from the more trusted inner layer, and deny all inbound requests from the less trusted outer layers ● Delete content after it is moved from the inbox / outbox storage. Consider the use of scripts to automatically delete content in the inbox / outbox storage after it has been there for a certain period of time, e.g. 24-48 hours. ● For facilities with sufficient resources, consider stronger separation of duties: requiring two different sets of individuals, one on the production side, and one on data I/O side, to move content from production to external networks ● Alternatively, hardware-encrypted hard drives using AES 256-bit encryption can be used to transfer data between production networks and data I/O systems, only if production and data I/O networks do not have any network connections and are different, physically separate VLANs (i.e., 'air gapped'). ● Exceptions: ○ Use of separate volumes for the inbox / outbox storage on the same SAN used for production is allowed if access to the data IO and production volumes can be restricted via layer 2/3 ACLs (Isilon, NetApp, etc.) ○ Other secure implementations may exist: e.g. dedicated inbox / outbox storage located in the production network, but only accessible from the data I/O network via a SMB proxy server that communicates across networks via strict layer 2/3 ACLs ○ Obtain client approval for other exceptions.	Google's controls for communication and network security are continuously reviewed and attested by Independent third party auditors in the following : ● AICPA/SOC 2 Controls: ● ISO/IEC 27001:2013: ● ISO/IEC 27017:2015: 15.1.1, 15.1.3 ● ISO/IEC 27018:2015: ● NIST SP 800-53 R3: ● PCI DSS v3.2: ● Shared Assessments (SIG) 2017 AUP: P.1 For more information, refer to the following: ● Google Infrastructure Security Design Overview. ● Google security whitepaper Google maintains one homogeneous operating environment for Google Cloud. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google intrusion detection involves: 1. Tightly controlling the size and make-up of Google's attack surface through preventative measures; 2. Employing intelligent detection controls at data entry points; and 3. Employing technologies that automatically remedy certain dangerous situations. See Row PS-6.1
DS-5.1	Block input/output (I/O), mass storage, external storage, and mobile storage devices (e.g., USB, FireWire, Thunderbolt, SATA, SCSI, etc.) and optical media burners (e.g., DVD, Blu-Ray, CD, etc.) on all systems that handle or store content, with the exception of systems used for content I/O. Refer to DS-4.0 for disconnecting wireless NICs. Implementation Guidance:	These external IO paths are disabled in the datacenters.

	• Consider the following for blocking I/O devices:
	  ○ Change the registry setting to restrict write access to I/O devices for MS Windows-based systems
	  ○ Remove the mass storage file to control write access on production stations for Mac-based systems
	  ○ Disable I/O devices using group policy for systems using Microsoft Active Directory or Apple Open Directory
	  ○ Use I/O port monitoring software to detect port usage if blocking output devices is not feasible
	• Write access to external devices is allowed if there is a valid business justification. Computers that allow write access to external devices must utilize an I/O port monitoring and logging solution.	

	XXXX. System Security	
DS-6.0	Install endpoint protection, and/or anti-virus and anti-malware software on all workstations, servers, and on any device that connects to production networks where content is stored (e.g., SAN/NAS etc.). This includes WFH and remote worker machines, along with VDI (virtual desktop infrastructure) used to access remote production networks. Implementation Guidance: • If a personal endpoint device (BYOD) is used and content is only accessed via a studio approved remote pixel streaming connection (e.g., PCoIP, RGS, Parsec, NICE DCV, etc.), with no content being download or uploaded, then this control should still be considered • Install an enterprise anti-virus and anti-malware solution with a centralized management console Consider the installation of endpoint protection • Consider the installation of endpoint protection or End Point Detection and Response (EDR), EPP (End Point Protection, or XDR (Extended Detection and Response) or MXDR (Managed Extended Detection and Response)	See Row PS-12.3 Google maintains an automated log collection and analysis tool to review and analyse log events. See Row DS-1.2
DS-6.1	Update all anti-virus and anti-malware definitions daily, or more frequently on all workstations, servers, WFH/Remote worker machines, and virtual desktops and servers. Implementation Guidance: • See DS-6.0 for applicability • Configure the centralized anti-virus and anti-malware management console to download and push definition updates at least once each day	Google defines a data security architecture conducive to its operational needs and has demonstrated that this architecture satisfies industry standards such as FedRamp, NIST 800-53, SOC 2/3 and ISO/IEC 27001 security objectives.
DS-6.2	Scan all content for viruses and malware prior to ingest onto the content / production network. Implementation Guidance: • Perform scans on a system that is not connected to the content / production network	See Row DS-6.1

	• To avoid impact on content / production systems, configure anti-virus and anti-malware software to only execute full file system scans during idle hours, non-business hours, and/or weekends.	
DS-6.2.1	Local firewalls should be implemented on workstations, including WFH, and remote worker machines, to restrict unauthorized access to the workstation. Implementation Guidance: • If content is not downloaded or uploaded by WFH and remote workers and is only accessed via a studio approved remote pixel streaming connection (e.g., PCoIP, RGS, Parsec, NICE DCV, etc.) and they are using a personal end point device (BYOD), then this control should still be considered. • Consider implementing on machines with higher security requirements that might also have access to the Internet (e.g. I/O machines, workstations used for Internet research etc.)	See Row DS-6.1
DS-6.3	Perform scans as follows: • Enable regular full system virus and malware scanning on all workstations • Enable full system virus and malware scans for servers and for systems connecting to a SAN/NAS Implementation Guidance: • Configure anti-virus and anti-malware software to conduct a full system scan based upon the anti-virus and antimalware strategy • Configure anti-virus and anti-malware software to execute during idle periods	See Row PS-12.3 See Row DS-1.2
DS-6.4	Implement a process to regularly update systems (e.g., file transfer systems, operating systems, databases, applications, network devices) with patches/updates that remediate security vulnerabilities. Implementation Guidance: • If content is not downloaded or uploaded by WFH and remote workers. and is only accessed via a studio approved remote pixel streaming connection (e.g., PCoIP, RGS, Parsec, NICE DCV, etc.) and they are using a personal end point device (BYOD), then this control should be considered • Where possible, implement a centralized patch management tool (e.g., WSUS, Shavlik, Altiris) to automatically deploy patches to all systems • Subscribe to security and patch notifications from vendors, other third parties, and security advisories • Apply critical patches as soon as they become available and within 48 hours on computers on externally accessible networks • Apply less critical patches in a timely manner, according to a defined cycle based on risk (e.g. monthly for medium, quarterly for low, etc.) • Test patches prior to deployment • Decommission legacy systems that are no longer supported	See Row PS-5.6

	• Implement an exception process and compensating controls for cases where there is a legitimate business case for not patching systems • Implement virtual patches using the IDS/IPS, where patches are unavailable for vulnerabilities, until a software patch is available	
DS-6.5	Prohibit users from being Administrators on their own workstations, unless required for software (e.g., ProTools, Clipster and authoring software such as Blu-Print, Scenarist and Toshiba). Documentation from the software provider must explicitly state that administrative rights are required. Implementation Guidance: • Ensure that the user account used to login to the workstation does not have privileges as an Administrator of the system	See Row PS-15.2
DS-6.6	Use cable locks on transportable computing devices that handle content (e.g., laptops, tablets, desktops, towers) when they are left unattended. Implementation Guidance: • Secure cable lock to a stationary object (e.g., table)	Google's defense in depth approach assumes that all devices may be compromised at any time. MFA on all systems prevents physical loss from compromising security. Physical security of all systems is built into the infrastructure.
DS-6.6.1	Apply seals or tamper evident stickers on cases used for all workstations and servers that receive, send, manipulate, or store content in the production network Implementation Guidance: • E.g. Data IO machines, to help secure the machines from physical tampering.	See Row DS-6.6
DS-6.7	Implement additional security controls for laptops and portable computing storage devices that contain content or sensitive information relating to client projects. Encrypt all laptops. Use hardware-encrypted portable computing storage devices. Install remote-kill software on all laptops/mobile devices that handle content to allow remote wiping of hard drives and other storage devices Implementation Guidance: • Attach privacy screens to laptops if they must be used in insecure locations • Do not connect laptops to any public wireless locations • Power down laptops when not in use, and do not make use of sleep or hibernation modes	See Row DS-10.5 See Row DS-11.1
DS-6.8	Restrict software installation privileges to IT management. Implementation Guidance: • Prohibit the installation and usage of unapproved software including rogue software (e.g., illegal or malicious software) • Scan all systems for an inventory of installed applications at least quarterly	Google uses automated configuration management tools, software release tools and mobile device management software to restrict and monitor the installation of unauthorized software.
DS-6.9	Implement security baselines and standards to configure corporate systems (e.g., laptops, workstations, servers, SAN/NAS, VDI (Virtual Desktop Infrastructure)) used at an onsite facility and for those used by WFH and remote workers.	Google maintains security configurations for its machines and networking devices. The configurations are maintained and serve as master copies for comparison against production instances. Deviations are identified and corrected.

	Implementation Guidance: Workstations within the production network should be hardened. Servers should also be hardened. The guidelines include but are not limited to: ● Disabling guest accounts and shares ● Installing endpoint protection, and/or anti-virus protection ● Enabling software firewalls ● Removing or disabling all unnecessary software ● Keeping software up to date ● Disabling remote connections ● Enabling the screen lock Develop a secure standard build that is used to image all systems	Google has automated mechanisms to detect deviations from the desired security configuration of its infrastructure. Google allows customers to use their own virtual image to use in Google Cloud, refer here for details.
DS-6.10	Unnecessary services and applications should be uninstalled from content transfer servers. Implementation Guidance: ● Review the list of installed services (e.g. services. MSc) on all content transfer servers and uninstall or disable any which are not required ● Review the list of installed applications on all content transfer servers and uninstall any which are not required ● Review the list of startup applications to ensure all nonessential applications are not running	See Row DS-6.1
DS-6.11	Maintain an inventory of systems and system components. Implementation Guidance: ● Update the inventory on at least a monthly basis	See Row PS-13.0
DS-6.11.1	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system. Include the use of cloud related software and services, along with the business purpose. Identify any software or cloud services that are not authorized. Implementation Guidance: ● Review list of software and cloud software and services on a quarterly basis and remove unauthorized software and cloud services and software ● Consider the use of a CASB (Cloud Access Security Broker) to monitor and restrict cloud software usage and access ● Notify and obtain approvals from content owners of any cloud services or software used	
DS-6.12	Document the network topology and update the diagram annually or when significant changes are made to the infrastructure.	Engineering teams maintain procedures to facilitate the rapid reconstitution of services. See Row DS-3.4

	Implementation Guidance: • Include WAN, DMZ, LAN, WLAN (wireless), VLAN, firewalls, and server/network topology	
	XXXXI. Account Management	

DS-7.0	Establish and implement an account management process for administrator, user, and service accounts for all information systems and applications that handle content.
	
	Implementation Guidance:
	• A Zero Trust Architecture should be adopted following NIST SP 800- 207 leveraging the following:
	  ○ At a minimum multi-factor authentication (MFA) for administrative accounts, and internet facing systems
	  ○ Identity and access management system
	  ○ Role based access control
	  ○ Single sign on system
	  ○ Identity federation standards
	• A directory service (e.g., Active Directory, Open Directory, LDAP) should be used for authentication to any infrastructure, shared storage, server, computer, or laptop device if there are more than 25 workstations.
	• Document policies and procedures for account management which address the following:
	  ○ New user requests User access modifications
	  ○ Disabling and enabling of user accounts
	  ○ User termination
	  ○ Account expiration
	  ○ Leaves of Absence
	  ○ Disallow the sharing of any user account by multiple users
	  ○ Restrict the use of service accounts to only applications that require them
	• Enable logging on the following infrastructure systems and devices at a minimum:
	  ○ Infrastructure components (e.g., firewalls, authentication servers, network operating systems, remote access mechanisms including VPN)
	  ○ Production operating systems
	  ○ Content management components (e.g., storage devices, content servers, content storage tools, content transport tools)
	  ○ Systems with Internet access
	  ○ Implement a server to manage the logs in a central repository (e.g., syslog/log management server, Security Information and Event Management (SIEM) tool)
		Google supports integration with a customer's SSO solution:
		
		• https://cloud.google.com/docs/permissions-overview
		• https://support.google.com/a/answer/6087519
		• https://support.google.com/a/answer/60224?hl= en&ref_topic=6348126
		
		Google supports open standards such as OAuth, OpenID and SAML 2.0. Google supports SAML as means for authenticating users. Google Cloud Identity & Access Management (IAM) lets administrators authorize who can take action on specific resources, giving you full control and visibility to manage cloud resources centrally. For established enterprises with complex organizational structures, hundreds of workgroups and potentially many more projects, Cloud IAM provides a unified view into security policy across your entire organization, with built-in auditing to ease compliance processes. IAM access policies are defined at the project level using granular controls of users and groups or using ACLs.
		
		• https://cloud.google.com/iam/
		• https://cloud.google.com/compute/docs/access/
		
		Customers can integrate authentication to G Suite to their existing identity management system. Customers can customize access to data by organization and user and assign administrative access profiles based on roles. Google provides the capability for domain administrators to enforce Google's 2-step verification. The 2nd factor could be a code generated by Google's Authenticator mobile application or via a supported hardware key. Should a tenant choose to set up SSO against their own password management system, they would be able to leverage any 3rd party multifactor option that their system supports Google supports integration with third-party identity assurance services.
		
		Custom policies can be enforced through SSO integration which is available as a standard part of our offering Google by default requires a password change upon first login Administrators can manually lock and unlock accounts.

DS-7.1	Maintain traceable evidence of the account management activities (e.g., approval emails, change request forms)	See Row PS-15.2 See Row DS-7.0

	Implementation Guidance: ● Retain evidence of management approvals and associated actions for all account management activities, where possible	
DS-7.2	Assign unique credentials on a need-to-know basis using the principles of least privilege. Implementation Guidance: ● WFH users should use unique credentials and not make these credentials accessible to other individuals (local as well as remote access accounts) ● Assign credentials on a need-to-know basis for the following information systems, at a minimum: ○ Production systems ○ Content management tools ○ Content transfer tools ○ Network infrastructure devices ○ Logging and monitoring systems ○ Client web portal ○ Account management systems (e.g., Active Directory, ○ Open Directory, LDAP) ○ VPN remote permissions, which should only be granted when absolutely required	See Row PS-15.2 See Row DS-7.0
DS-7.3	Rename the default administrator accounts and other default accounts and limit the use of these accounts to special situations that require these credentials (e.g., operating system updates, patch installations, software updates). Implementation Guidance: ● This also applies to WFH and remote workers users on equipment, such as firewalls, WIFI, and routers, etc., if they are accessing or storing content ● Consult the documentation for all hardware and software to identify all of the default account(s) ● Change the password for all default accounts ● Where possible, change the user name for each account ● Disable administrator accounts when not in use	All accounts on production systems are tightly controlled. See Row PS-16.4 See Row PS-6.2
DS-7.4	Segregate duties to ensure that individuals responsible for assigning access to information systems are not themselves end users of those systems (i.e., personnel should not be able to assign access to themselves). Implementation Guidance: ● Leverage an independent team to grant access to information systems when possible ● Implement compensating controls when segregation is unattainable, such as: ○ Monitor the activity of company personnel and third party workers ○ Retain and review audit logs ○ Implement physical segregation	See Row PS-6.1

	○ Enforce management supervision	
DS-7.5	Monitor and audit administrator and service account activities. Implementation Guidance: ● Enable monitoring controls for systems and applications which support logging ● Configure systems and applications to log administrator actions and record, at the minimum, the following information: ○ User name ○ Time stamp ○ Action ○ Additional information (action parameters) ● Monitor service accounts to ensure that they are used for intended purposes only (e.g., database queries, application-to-application communication) ● Implement a monthly process to review administrator and service account activity to identify unusual or suspicious behavior and investigate possible misuse	See Row PS-12.3
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. Implementation Guidance: ● Remove access rights to information systems from users that no longer require access due to a change in job role or termination of company personnel and/or third party workers. ● Review user access on the following: ○ Key applications (content management, inventory, etc.) ○ Project folders, data I/O inbox / outbox, and centralized storage ○ Network communications devices (firewalls, routers, switches, etc.) ● Change shared account (administrator, root) passwords when persons who know those passwords no longer require access ● Remove or disable accounts that have not been used in over 90 days	See Row PS-6.2
DS-7.7	Restrict user access to content on a per-project basis. Implementation Guidance: ● Remove access rights to information systems from users that no longer require access due to project completion	See Row PS-16.4
DS-7.8	Disable or remove local accounts on systems that handle content where technically feasible. Implementation Guidance: ● Implement a centralized account management server (i.e., directory server such as LDAP or Active Directory) to authenticate user access to information systems ● For network infrastructure devices, implement Authentication, Authorization, and Accounting (AAA) for account management	All accounts on production systems are tightly controlled. See Row DS-6.1

	• Disable the guest account • If local accounts must be used, where possible, change the user name and password for each default account, disable the ability to logon to the system through the network using local accounts	
	XXXXII. Authentication	
DS-8.0	Enforce the use of unique usernames and passwords to access information systems Implementation Guidance: • Establish policies to enforce the use of unique usernames and passwords for all information systems • Configure information systems to require authentication, using unique usernames and passwords at a minimum	See Row DS-10.8 See Row PS-15.2 See Row DS-7.0
DS-8.1	Enforce a strong password policy for gaining access to information systems. Password policy should include guidance for service accounts. Utilize MFA for all administrative accounts, any internet facing systems. MFA should be utilized by remote and WFH users when connecting to corporate and/or production systems. Implementation Guidance: A facility should opt to choose one or more of the following password policies (A to C, listed in order of most preferred) for user accounts for employees, guests, contractors, and/or vendors. For administrative accounts, internet facing systems, and when remote/WFH users are connecting to corporate and/or production systems MFA must be implemented in option A): A. Utilize multi-factor authentication (MFA) that uses a combination of two or more of the following: 1. Something they know and only they know (e.g. password) 2. Something they have and only they have (e.g. soft or hard token) 3. Something they and only they are (e.g. biometrics) B. Password policies that are able to demonstrate the implementation of all the following criteria based on NIST 800-63b: 1. Password length is at least 12 characters 2. Passwords cannot contain common names or dictionary names (e.g. password1234, companyname!, firstnamelastname1) and should be enforced via a password black list 3. Password lockout must occur after 5 invalid attempts and can be automatically locked out after 1 minute 4. A manual password reset must require the password to be changed after the next successful login 5. All passwords hashes are reviewed quarterly for weaknesses via password cracking tools 6. Hashes are run through cracking tools for a minimum of 24 hours 7. The password black list is updated quarterly	See Row DS-10.8 See Row PS-15.2 See Row DS-7.0

	8. Passwords that are cracked must be added to the black list and changed within 30 days C. Create a password policy that consists of the following: 1. Minimum password length of 12 characters 2. Minimum of 3 of the following parameters: upper case, lower case, numeric, and special characters 3. Maximum password age of 365 days 4. Minimum password age of 1 day 5. Maximum invalid logon attempts of between 3 and 5 attempts 6. User accounts locked after invalid logon attempts must be manually unlocked, and should not automatically unlock after a certain amount of time has passed 7. Password history of ten previous passwords D. Service accounts unable to comply with A) to C) should adhere to the following criteria at a minimum: 1. Restrict access to only what is needed for services 2. Minimum password length of 12 characters 3. Minimum of 3 of the following parameters: upper case, lower case, numeric, and special characters 4. Maximum invalid logon attempts of between 3 and 5 attempts 5. Monitoring and alerts of the following activities via central logging: i. Successful login ii. Failed logon due to bad password or user name iii. Failed logon due to account lockout iv. Failed logon due to inadequate rights v. Review of activity on a monthly basis vi. Changing of passwords upon detection of suspicious activity 6. Consider the use of a Privileged Account Management (PAM) tool	
DS-8.2	For remote access (e.g., VPN) to the networks, implement two-factor authentication (e.g., username / password and hard token) and monitor activity. Implementation Guidance: ● WFH users must also ensure that VPN or other remote connections (e.g., PCoIP, RGP, etc.) utilizes MFA authentication ● Require individuals to provide two of the following for remote access: ○ Information that the individual knows (e.g., username, password) ○ A unique physical item that the individual has (e.g., token, keycard, smartphone, certificate) ○ A unique physical quality/biometrics that is unique to the individual (e.g., fingerprint, retina) ● Use two-factor authentication and a VPN connection with advanced encryption standard (AES-256) to carryout remote administration functions ● Review remote access VPN logins and activity on at least a monthly basis	See Row PS-15.2

DS-8.2.1	Implement two-factor authentication (e.g., username / password and hard token / verification code text message) for access to web based e-mail (Google, Microsoft, etc.) from desktops or mobile computing devices. Implementation Guidance: ● If smartphone access to e-mail s is not necessary, consider blocking webmail from smartphones to force desktop access ● Do not use personal accounts - use corporate accounts on enterprise offerings ● Web based e-mail services should have virus and malware protection	See Row PS-15.2 See Row DS-7.0
DS-8.3	Implement password-protected screen savers or screen lock software for servers and workstations. Implementation Guidance: ● WFH and remote users should ensure that any workstation or device used for work, has a password-protected screenlock ● Configure servers and workstations manually or via a policy (such as Active Directory group policies) to activate a password-protected screensaver after a maximum of 10 minutes of inactivity	Google's Device Policy Manager requires personnel to set an automatic lockout screen.
DS-8.4	Consider implementing additional authentication mechanisms to provide a layered authentication strategy for WAN and LAN / Internal Network access. Implementation Guidance: ● Authentication and authorization methods should leverage Zero Trust Architecture, as referred in NIST SP 800-207. ● Consider adding one or more of the following: ○ Multi-factor authentication ○ Identity and access management system ○ Single sign on system ○ Identity federation standards	See Row DS-7.0
	XXXXIII. Logging and Monitoring	
DS-9.0	Implement real-time logging and reporting systems to record and report security events; gather the following information at a minimum: When (time stamp) Where (source) Who (user name) What (content) Implementation Guidance: ● Enable logging on the following infrastructure systems and devices at a minimum: ○ Infrastructure components (e.g., firewalls, authentication servers, network operating systems, remote access mechanisms (e.g., VPN systems) ○ Production operating systems ○ Content management components (e.g., storage devices, content servers, content storage tools, content transport tools)	See Row PS-10.2

	○ Systems with Internet access Applications	
DS-9.01	Implement logging mechanisms on all systems used for the following: ● Key generation ● Key management ● Vendor certificate management Implementation Guidance: ● Ensure that all generated keys and added certificates are traceable to a unique user	Google's use and management of encryption keys is transparent to customers. Encryption keys may be applied to a customer, a file, disk, or transaction level depending on the type of encryption employed. Google has a service (External Key Manager) that allows customers to supply their own encryption keys via API. Customers can choose to store and manage encryption keys in a third-party key management system deployed outside Google's infrastructure. External Key Manager works with Cloud KMS and enables the separation between customers' data at rest and the encryption keys for supported services. Refer to the following resources: ● For more details on the External Key Manager, refer here ● For more details on Cloud KMS, refer here Google maintains internal documentation for the use of its internal proprietary key management service.
DS-9.1	Implement a server to manage the logs in a central repository (e.g., syslog/log management server, Security Information and Event Management (SIEM) tool).	See Row DS-6.1
DS-9.2	Configure logging systems to send automatic notifications when security events are detected in order to facilitate active response to incidents. Implementation Guidance: ● Define events that require investigation and enable automated notification mechanisms to appropriate personnel; consider the following: ○ Successful and unsuccessful attempts to connect to the content / production network ○ Unusual file size and/or time of day transport of content Repeated attempts for unauthorized file access ○ Attempts at privilege escalation ● Implement a server to aggregate logs in a central repository (e.g., syslog/log management server, Security Information and Event Management (SIEM) tool)	See Row DS-3.4 See Row PS-10.3 See Row DS-9.3
DS-9.3	Investigate any unusual activity reported by the logging and reporting systems. Implementation Guidance: ● Incorporate incident response procedures for handling detected security events	Google has a well defined and rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Google's security incident management program is structured around the NIST guidance on handling incidents (NIST SP 800–61). Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Google requires its employees to report immediately, all known or suspected information security and privacy incidents (defined as "Data Incidents" below) to the Security and Privacy Incident Management team. For more details, refer section 7.2 of Google's Cloud Data Processing Addendum.

		Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Additionally, Google communicates outage information through its status dashboards: ● For Google Cloud: ● For Google Workspace: Due to the fact that the incident response system is standardized, customization of the notification process is not supported for each tenant. The terms of service cover roles and responsibilities. Google performs annual testing of its emergency response processes. Google reviews and analyzes security incidents to determine impact, cause and opportunities for corrective action. The amount of security incident data is currently statistically insignificantly small. Should the amount of data increase, Google will consider sharing this statistical information. Google's end-to-end data incident response process is described in this whitepaper
DS-9.4	Review all logs weekly, and review all critical and high daily. Implementation Guidance: ● Investigate any unusual activity that may indicate a serious security incident ● Identify any additional unusual events that are not currently being alerted on and configure the logging and reporting system to send alerts on these events ● Correlate logs from different systems to identify patterns of unusual activity ● Based on findings of log reviews, update SIEM settings as appropriate	See Row DS-9.3
DS-9.5	Enable logging of internal and external content movement and transfers and include the following information at a minimum: ● Username ● Timestamp ● File name ● Source IP address ● Destination IP address ● Event (e.g., download, view)	See Row DS-9.3
DS-9.6	Retain logs for at least one year. Implementation Guidance: ● Seek guidance from legal counsel to determine any regulatory requirements for log retention ● Store content logs on a centralized server that can be accessed only by specific users and is secured in an access-controlled room	See Row DS-9.3

DS-9.7	Restrict log access to appropriate personnel. Implementation Guidance: ● Maintain Access Control Lists to ensure that only personnel responsible for log monitoring and review have permission to view logs ● Segregate duties to ensure that individuals are not responsible for monitoring their own activity ● Protect logs from unauthorized deletion or modification by applying appropriate access rights on log files	See Row PS-15.2
	XXXXIV. Mobile Security	
DS-10.0	Define security controls and standards for mobile computing devices. Refer to MS-4.0.2 for mobile computing device policies. Implementation Guidance: ● Consider implementing the following mobile computing device security controls and standards: ○ antivirus/anti-malware protection ○ inactivity lock (PIN, swipe, fingerprint) ○ data wipe after successive invalid attempts to unlock ○ data encryption ○ patching and OS revision management ○ remote data wipe ○ centralized mobile device management ○ approved models	Google maintains a mobile policy and provides detailed instructions to personnel that wish to provision access to Google services on their mobile device. The policy includes eligibility requirements and security policy requirements.
DS-10.1	Develop a list of approved applications, application stores, and application plugins/extensions for mobile devices accessing or storing content. Implementation Guidance: ● Prohibit the installation of non-approved applications or approved applications that were not obtained through a pre-approved application store ● Consider a mobile device management system	The Google Device Policy restricts the user and device behavior on mobile devices including application installation. For advanced use, a Work Profile is required which includes a restricted Apps Store. Google's Device Policy does not permit the use of third party application stores.
DS-10.2	Maintain an inventory of all mobile devices that access or store content. Implementation Guidance: ● Include operating system, patch levels, applications installed	All devices must register through the Google Device Policy Manager unless browser-only access is used. Google's Device Policy Manager enforces Google's mobile policy except when access is solely to Apps services and through a browser.
DS-10.3	Require encryption either for the entire device or for areas of the device where content will be handled or stored. Implementation Guidance: ● Consider a mobile device management system	Mobile devices with access to corporate resources other than Apps services require encryption.

DS-10.4	Prevent the circumvention of security controls. Implementation Guidance: • Prevent the use of jailbreaking, rooting etc	Google's mobile policy does not permit jailbreaking or rooting on devices linked to a Google corporate account. Google's Device Policy Manager may not install on a device that does not conform to the required security specifications. The Device Policy Manager is required in order to access corporate sources using mobile applications
DS-10.5	Implement a system to perform a remote wipe of a mobile device, should it be lost / stolen / compromised or otherwise necessary. Implementation Guidance: • Remind employees that non-company data may be lost in the event a remote wipe of a device is performed	Google's supports remote wipe capabilities for mobile devices with access to sensitive corporate information.
DS-10.6	Implement automatic locking of the device after 10 minutes of non-use.	See Row DS-8.3.
DS-10.7	Manage all mobile device operating system patches and application updates. Implementation Guidance: • Apply the latest available security-related patches/updates upon general release by the device manufacturer, carrier or developer	The management of O/S levels is the responsibility of the user. Google's mobile policy requires the installation of all updates and sets minimum O/S requirements.
DS-10.8	Enforce password policies. Implementation Guidance: • Refer to DS-8.1 • Use biometrics (fingerprint reader)	Google's Device Policy Manager enforces password policies. Devices are assigned minimum password requirements that cannot be circumvented by the user.
DS-10.9	Consider implementing a system to perform backup and restoration of mobile devices. Implementation Guidance: • Encrypt backups and store them in a secure location	Data from Google services are synced from the cloud data store to the device. Google's mobile device policy does not permit the use of unapproved application stores. Google's mobile device policy requires all mobile devices (including personally owned devices) to conform to corporate device management policies that apply restrictive controls to reduce the risk of malware based attacks.
	XXXXV. Security Techniques	
DS-11.0	Ensure that security techniques (e.g., spoiling, invisible/visible watermarking) are available for use and are applied when instructed.	See Row DS-6.1
DS-11.1	Encrypt content on hard drives or encrypt entire hard drives using a minimum of AES-256 encryption by either: • File-based encryption: (i.e., encrypting the content itself) • Drive-based encryption: (i.e., encrypting the hard drive) Implementation Guidance: • Drives used by WFH and remote workers to store content must be encrypted • For all (internal, external) hard drives, consider purchasing pre-encrypted drives (e.g., Rocstor Rocsafe, LaCie Rugged Safe, Apricorn) • The use of external hard drives should be approved by the client prior to use. Single factor authentication is allowed only if the authentication is a keypad pin. Without a keypad pin authentication, consider using client approved encryption solutions.	We encrypt data at rest in Google Cloud. Network packets are encrypted when they leave Google Compute Engine Instances. Google has a service (External Key Manager) that allows customers to supply their own encryption keys via API. Customers can choose to store and manage encryption keys in a third-party key management system deployed outside Google's infrastructure. External Key Manager works with Cloud KMS and enables the separation between customers' data at rest and the encryption keys for supported services. Resources: • For more details on the External Key Manager, refer here • For more details on Cloud KMS, refer here • For details on Encryption of Data at Rest, refer here • For details on Encryption of Data in Transit, refer here

	• Drives with keypad pin authentication should enforce limited invalid authentication attempts after which content stored on the drives is erased or the drives self-destruct.
	• Encrypt all content on hard drives including:
	  ○ SAN / NAS
	  ○ Servers
	  ○ Workstations
	  ○ Desktops
	  ○ Laptops
	  ○ Mobile devices
	  ○ External storage drives
	• Implement one or more of the following:
	  ○ File-based encryption such as encrypted DMGs or encrypted ZIP files
	  ○ Drive-based encryption using software
		Google maintains internal documentation for the use of its internal proprietary key management service.

DS-11.2	Send decryption keys, keypad pins, or passwords using an out-of-band communication protocol (i.e., not on the same storage media as the content itself). Implementation Guidance: • Send decryption keys or passwords using a different method than that which was used for the content transfer • Check to ensure key names and passwords are not related to the project or content	See Row DS-11.5 See Row DS-11.1
DS-11.3	Implement and document key management policies and procedures: • Use of encryption protocols for the protection of sensitive content or data, regardless of its location (e.g., servers, databases, workstations, laptops, mobile devices, data in transit, email) • Approval and revocation of trusted devices • Generation, renewal, and revocation of content keys • Internal and external distribution of content keys • Bind encryption keys to identifiable owners • Segregate duties to separate key management from key usage • Key storage procedures • Key backup procedures Implementation Guidance: • Consider the creation of unique encryption keys per client and for critical assets • Prevent unauthorized substitution of cryptographic keys • Require cryptographic key custodians to formally acknowledge that they understand and accept their key custodian responsibilities	Google maintains documentation on its key management process and provides controls to manage encryption keys through their lifecycle and protect against unauthorized use.
DS-11.4	Encrypt content at rest and in motion, including across virtual server instances, using a minimum of AES-256 encryption. Implementation Guidance:	See Row DS-11.1

	• "http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf"	
DS-11.5	Store secret and private keys (not public keys) used to encrypt data/content in one or more of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (e.g., Host Security Module (HSM) or a Pin Transaction Security (PTS) point-of-interaction device) ○ Has at least two full-length key components or key shares, in accordance with a security industry accepted method	Google uses a combination of open source and proprietary encryption formats and algorithms validated by Google security engineers. Google maintains its own encryption keys. Google stores its keys in its own production environment. Google's key management operates as a service for engineering teams to use in their application code.
DS-11.6	Confirm that devices on the Trusted Devices List (TDL) are appropriate based on rights owners' approval. Implementation Guidance: • Require clients to provide a list of devices that are trusted for content playback • Only create Key Delivery Messages (KDMs) for devices on the TDL	Google maintains a mobile device policy that details our requirements for mobile device use at Google. Customer data is not permitted on mobile devices.
DS-11.6.1	Access to KDMs must be restricted to the KDM creator and exhibitor only.	See Row DS-6.1
DS-11.6.2	KDM creation and handling must be physically and digitally segregated from DCP handling and replication where feasible	See Row DS-6.1
DS-11.7	Encrypt content at rest and in motion, including across virtual server instances, using a minimum of AES-256 encryption. Implementation Guidance: • Require clients to provide expiration dates for content keys • Specify an end date for when keys expire to limit the amount of time for which content can be viewed	See Row DS-6.1
	XXXXVI. Content Tracking	
DS-12.0	Implement a digital content management system to provide detailed tracking of digital content. Implementation Guidance: • Log all digital content that is checked-in/checked-out • Log the digital location of all content • Log the expected duration of each check-out • Log the time and date of each transaction	See Row DS-6.1.
DS-12.1	Retain digital content movement transaction logs for one year. Implementation Guidance: • Include the following: ○ Time and date of check-in/check-out ○ Name and unique id of the individual who checked out an asset ○ Reason for check-out	See Row DS-6.1.

	○ Location of content	
DS-12.2	Review logs from digital content management system periodically and investigate anomalies.	See Row DS-6.1.
DS-12.3	Use client AKAs (“aliases”) in asset tracking systems, unless otherwise as directed by the client. Implementation Guidance: ● Restrict knowledge of client AKAs to personnel involved in processing client assets	See Row DS-6.1.
DS-12.4	Use enterprise (not personal) versions of online or web based collaboration services (e.g., Google Docs, etc.) for tracking content, managing inventory, or workflow management, Utilize multi-factor authentication and centrally managed user accounts and access to data. Implementation Guidance: ● Implement two-factor authentication ● Subscribe to enterprise or corporate editions to allow centralized management of users and access to data ● Review user accounts and access to data and files on a quarterly basis (refer to DS-7.6) ● Implement a periodic process to purge old data and files	See Row DS-6.1.
	XXXXVII. Transfer Systems	
DS-13.0	Use only client-approved transfer systems that utilize access controls, a minimum of AES-256 encryption for content at rest and for content in motion and use strong authentication for content transfer sessions. Implementation Guidance: ● WFH users and remote workers should only use client approved transfer systems ● Allow only authorized users to have access to the content transfer system ● Consider restricting access also on a project basis ● Verify with the client that the content transfer systems are approved, prior to use	See Row DS-6.1.
DS-13.1	Implement an exception process, where prior client approval must be obtained in writing, to address situations where encrypted transfer tools are not used. Implementation Guidance: ● Use randomly generated usernames and passwords that are securely communicated for authentication ● Use only client-approved transfer tools / application ● Require clients to sign off on exceptions where unencrypted transfer tools must be used ● Document and archive all exceptions	See Row DS-6.1.

	XXXXVIII. Transfer Device Methodology	
DS-14.0	Implement and use dedicated systems for content transfers. Implementation Guidance: • Ensure editing stations and content storage servers are not used to directly transfer content • Disable VPN/remote access to transfer systems, or to any system used to store, transfer or manipulate content • Create an approval process to authorize the transfer of content • Create and maintain a list of users who are responsible for transferring content to and from the production network • Create and maintain a log of other facilities (within a vendor's company or otherwise) to which content is digitally transferred for additional service fulfillment or storage. The log should include the company's name, address, key contact person, phone number, and email address • Track which machines are dedicated servers / workstations for transferring content and noting the location of these machines • Use an approval process that checks for proper authentication • Use work orders that assign operators access to digital transfer systems prior to placing files for delivery • Conduct regular reviews of who may access the transfer services. This includes, but is not limited to, removing access for completed projects, inactive accounts, and file / directory permissions. Such reviews should occur every three months at a minimum	See Row DS-6.1.
DS-14.1	Separate content transfer systems from administrative and production networks. Implementation Guidance: • Separate networks either physically or logically.	See Row DS-6.1.
DS-14.2	Place content transfer systems in a Demilitarized Zone (DMZ) and not in the content / production network. Implement whitelisting on content transfer servers to only allow transfers to and from authorized external transfer servers. Implementation Guidance: • Harden content transfer systems prior to placing them in the DMZ (refer to DS-1.5 for suggestions) • Implement Access Control Lists (ACLs) that restrict all ports other than those required by the content transfer tool • Implement ACLs to restrict traffic between the internal network and the DMZ to specific source/destination IP addresses • If FQDN (Fully Qualified Domain Names) are used, the firewall should contain a valid DNS entry. DNS resolution should be confirmed it is refreshing periodically to ensure the latest IP addresses are captured in the ACL	See Row DS-6.1.

	• Disable access to the Internet from the systems used to transfer content, other than the access needed to download client content or to access approved content transfer locations • Review and update white listings quarterly	
DS-14.3	Remove content from content transfer devices/systems immediately after successful transmission/receipt. Implementation Guidance: • Require clients to provide notification upon receipt of content • Implement a process to remove content from transfer devices and systems, including from recycle bins • Where applicable, remove client access to transfer tools immediately after project completion • Confirm the connection is terminated after the session ends	This falls under the shared security model and is the customer's responsibility to configure their client systems in a compliant manner.
DS-14.4	Send automatic notifications to the production coordinator(s) upon outbound content transmission. Implementation Guidance: • Configure the content transfer system to send an automatic notification (e.g., an email) to the production coordinator(s) each time a user sends content out of the network	See Row DS-14.3
	XXXXIX. Client Portal	
DS-15.0	Restrict access to web portals which are used for transferring content, streaming content and key distribution to authorized users. Implementation Guidance: Implement access control measure around web portals that transfer content, stream content and distribute keys by implementing one or more of the following: • Require user credentials • Integrate machine and/or user keys for authentication and authorization • Manage encryption keys using proper segregation of duties (e.g., one person should create the keys and another person should use the keys to encrypt the content) • Limit portal access to specific networks, VLANs, subnets, and/or IP address ranges • Restrict the ability to upload/download as applicable from the client portal	This is outside the scope of Google and falls under customer responsibility.
DS-15.1	Assign unique credentials (e.g., username and password) to portal users and distribute credentials to clients securely Implementation Guidance: • Do not embed user names and passwords in content links • Consider distributing the user credentials and content links in separate emails	See Row DS-15.0

	• Consider distributing user credentials via phone or SMS • Consider distributing encryption keys via out of band transfer	
DS-15.2	Ensure users only have access to their own digital assets (i.e., client A must not have access to client B's content). Implementation Guidance: • Implement a process to review file/directory permissions at least quarterly • Ensure that access is restricted to only those that require it	See Row DS-15.0
DS-15.3	Place the web portal on a dedicated server in the DMZ and limit access to/from specific IPs and protocols. Implementation Guidance: • Implement Access Control Lists (ACLs) that restrict all ports other than those required by the client portal • Implement ACLs to restrict traffic between the internal network and the DMZ to specific source/destination IP addresses • Harden systems prior to placing them in the DMZ (refer to DS-1.5 for suggestions)	See Row DS-15.0

DS-15.4	Prohibit the use of third-party production software/systems/services that are hosted on an internet web server unless approved by client in advance.
	
	Implementation Guidance:
	• Consider adding one or more of the following:
	  ○ Multi-factor authentication
	  ○ Identity and access management system
	  ○ Single sign on system
	  ○ Identity federation standards
	  ○ Use a VPN connection with advanced encryption standard (AES-256)
		See Row DS-15.0

DS-15.5	Use HTTPS and enforce the use of a strong cipher suite (e.g., TLS v1.3) for the internal/external web portal. Acquire an HTTPS public key certificate signed by a certificate authority trusted by a majority of web browsers. Implementation Guidance: • Ensure certificates are up to date and not expired • Avoid the use of self-signed certificates	See Row DS-6.1
DS-15.6	Do not use persistent cookies or cookies that store credentials in plaintext. Implementation Guidance: • Review the use of cookies by existing web-based applications and ensure none of them store credentials in plaintext • If an application is storing credentials in plaintext cookies then take one of the following actions:	See Row DS-6.1

	○ Reconfigure the application Update the application ○ Request a security patch from the application developer	
DS-15.7	Set access to content on internal or external portals to expire automatically at predefined intervals, where configurable.	See Row DS-15.0
DS-15.8	Test for web application vulnerabilities quarterly and remediate any validated issues. Implementation Guidance: ● Vulnerability scans should include Application Programming Interface (API)s ● Consider use of both authenticated and unauthenticated scanning ● Use industry accepted testing guidelines, such as those issued by the Open Web Application Security Project (OWASP) to identify common web application vulnerabilities such as Cross Site Scripting (XSS), SQL Injection, and Cross Site Request Forgery (CSRF) ● Testing should be performed by an independent third party	See Row DS-15.0
DS-15.9	Perform annual penetration testing of web applications and remediate any validated issues. Implementation Guidance: ● Penetration testing should include Application Programming Interface (API)s ● Consider use of both authenticated and unauthenticated testing ● Use industry accepted testing guidelines, such as those issued by the Open Web Application Security Project (OWASP) to identify common web application vulnerabilities such as Cross Site Scripting (XSS), SQL Injection, and Cross Site Request Forgery (CSRF) ● Testing should be performed by an independent third party	See Row DS-15.0
DS-15.10	Allow only authorized personnel to request the establishment of a connection with the telecom service provider.	See Row DS-15.0
DS-15.11	Prohibit transmission of content using email (including webmail). Implementation Guidance: ● Consider the use of secure email appliance servers to encrypt emails and attachments (e.g., Cisco IronPort, Sophos E-Mail Security Appliance, Symantec PGP Universal Gateway Email)	See Row DS-15.0
DS-15.12	Review access to the client web portal at least quarterly. Implementation Guidance: ● Remove access rights to the client web portal once projects have been completed ● Remove any inactive accounts ● Consider sending automatic email notifications to an appropriate party whenever data is transferred	See Row DS-15.0

DS-15.13	Implement a process to review the facility's public informational website and other online industry resources for sensitive information that could be leveraged by an attacker (e.g. mentions of internal infrastructure and technologies, content transfer servers, IP addresses, photos of sensitive areas, current content being worked on, etc.) Implementation Guidance: ● Implement a change control / approval process and/or tool before content can be added to or modified on the public informational website. ● Review IMDb, LinkedIn, etc.	See Row DS-15.0