Google Cloud

MPAA - Google Cloud Platform - Compliance Mapping

This document details the Motion Picture Association of America (MPAA) controls that Google Cloud complies with.

No.	Security Topic	Best Practice	Google Implementation	Implementation Guidance	CSA 3.01 Mapping
MS-1.0	Executive Security Awareness/ Oversight	Establish an information security management system that implements a control framework for information security which is approved by the business owner(s) /senior management.	Google conducts rigorous internal continuous testing of our application surface through various types of penetration exercises. In addition, Google coordinates external 3rd party penetration testing using qualified and certified penetration testers.	· e.g., ISO27001's ISMS Framework, NIST, CoBIT, etc.	
MS-1.1		Review information security management policies and processes at least annually.	Google makes its SOC 2/3 report and ISO 27001 certificate available to customers. Google's security teams are committed to a strong perimeter and dedicated staff are responsible for the safety and security of Google's network infrastructure. Google conducts rigorous internal continuous testing of our network perimeter through various types of penetration exercises. In addition, Google coordinates external 3rd party penetration testing using qualified and certified penetration testers. Google conducts rigorous internal continuous testing of our application surface through various types of penetration exercises. In addition, Google coordinates external 3rd party penetration testing using qualified and certified penetration testers. Google maintains an internal audit program consistent with industry best practices and regulatory requirements. Google is committed to maintaining a program where independent verification of security,		AAC-02 AAC-03 GRM-09

			privacy and compliance controls are regularly reviewed. 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 27001 ISO 27017 / 27018 PCI-DSS HIPAA Google Security Policy prohibits sharing this information but customers may conduct their own testing on our products and services. Google publishes and makes available its ISO 27001, 27017, 27018 and SOC3 reports online. Detailed information of some confidential reports can be obtained under NDA. 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. Customer data is logically segregated by domain to allow data to be produced for a single tenant only. However, it is the responsibility of the customer to deal with legal requests. Google will provide customers with assistance with these requests, if necessary. Google has built multiple redundancies in its systems to prevent permanent data loss. Data durability assurances are built in the the service specific terms as part of the the terms of service. https://cloud.google.com/terms/service-terms Customers can choose data location in US and Europe when configuring some their Google Cloud Platform services. If these selections are made around choice of data location this is backed by the service specific terms within Google's Terms of Service. https://cloud.google.com/terms/service-terms		

			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 customer for changes. 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-1.2		Train and engage executive management/owner(s) on the business' responsibilities to protect content at least annually.	At Google, managers are responsible for ensuring their direct reports complete the required trainings and affidavits. Google maintains a robust vendor management program. Vendors who work with Google are required to comply with all relevant information security and privacy policies. In addition, Google has open-sourced its vendor management questionnaires for use by the community: https://opensource.googleblog.com/2016/03/scalable-vendor-security-reviews.html		GRM-03 GRM-05
MS-1.3		Create an information security management group to establish and review information security management policies.	Google's security teams are committed to a strong perimeter and dedicated staff are responsible for the safety and security of Google's network infrastructure. Google's security team consists of over 700 individuals. Google conducts rigorous internal continuous testing of our network perimeter through various types of penetration exercises. In addition, Google coordinates external 3rd party penetration testing using qualified and certified penetration testers.		
MS-2.0	Risk Management	Develop a formal, documented	Google Cloud platform provides the ability to log and monitor security and system health.	· Define a clear scope for the security risk	GRM-02 GRM-08

		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.	https://cloud.google.com/docs/ Google performs risk assessments as required by ISO 27001. 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. Google performs risk assessments as required by ISO 27001.	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 · Refer to MS-6.0 for best practices regarding documented workflows	GRM-10
MS-2.1	Risk Management	Conduct an internal risk assessment annually and upon key workflow changes—based on, at a minimum, the MPAA Best Practice Common Guidelines and the applicable Supplemental Guidelines—and document and act upon identified risks.	Google performs periodic network vulnerability scans using commercial tools. Google performs periodic application-layer vulnerability scans using commercial and proprietary tools. Google performs periodic 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 monitor 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 guides. https://cloud.google.com/security/whitepaper https://cloud.google.com/terms/ Google Cloud platform provides the ability to log and monitor security and system health. https://cloud.google.com/docs/ Google performs risk assessments as required by ISO 27001.	· Conduct meetings with management and key stakeholders at least quarterly to identify and document content theft and leakage risks · Conduct quarterly 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 · Monitor and assess the effectiveness of remediation efforts and implemented controls at least quarterly · Document and budget for security initiatives, upgrades, and maintenance	TVM-02 GRM-02 GRM-11

			Google has documented its risk management procedures as part of its ISMS that underlies our ISO 27001 certification. Google has documented its risk management procedures as part of its ISMS that underlies our ISO 27001 certification. Documentation is made available to all individuals that may participate in or need to be informed of risk management and assessment programs.		
MS-3.0	Security Organization	Identify security key point(s) of contact and formally define roles and responsibilities for content and asset protection.	Google monitors a variety of communication channels for security incidents, and Google's security personnel will react promptly to known incidents. Google's Terms of Service outline the responsibilities of Google and customers.	· 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	SEF-01 HRS-07
MS-4.0	Policies and Procedures	Establish policies and procedures regarding asset and content security; policies should address the following topics, at a minimum: · Acceptable use (e.g., social networking, Internet, phone, personal devices, mobile devices, etc.) · Asset and content classification and handling policies · Business continuity	Google provides security awareness training to all employees that include reference to our security policies which include our mobile policy. 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. https://cloud.google.com/compute/docs/label-or-tag-resources Google tags physical hardware. Components are inventoried for easy identification and tracking within Google facilities. Other	· 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 F for a list of policies and procedures to consider	MOS-05 DSI-01 BCR-01 BCR-03 BCR-11

		(backup, retention and restoration) · Change control and configuration management policy · Confidentiality policy · Digital recording devices (e.g., smart phones, digital cameras, camcorders) · Exception policy (e.g., process to document policy deviations) · Incident response policy · Mobile device policy · Network, internet and wireless policies · Password controls (e.g., password minimum length, screensavers) · Security policy · Visitor policy · Disciplinary/Sanction policy · Internal anonymous method to report piracy or mishandling of content (e.g., telephone hotline or email address)	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. Google may store customer data is the following locations: http://www.google.com/about/datacenters/inside/locations/ Customers can apply their own data-labeling standard to information stored in Google Cloud Platform. Many Cloud Platform 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 https://cloud.google.com/terms/service-terms Google operates a global network of data centers to reduce risks from geographical disruptions. The link below includes the locations of our data centers: http://www.google.com/about/datacenters/inside/locations/ 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. The Google datacenter network infrastructure is secured, monitored, and environmentally controlled. Due to the dynamic and sensitive nature of this information, Google does not share this information with tenants. 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. Customers need to manage this by leveraging the features of our storage services. Please see the product documentation for specifics: https://cloud.google.com/docs/storing-your-data		

			Customers are primarily responsible for legal requests. Google will assist customers where necessary. Google's process for handling law enforcement requests is detailed here: http://www.google.com/transparencyreport/userdatarequests/legalprocess/ 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. However, 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.		
MS-4.1	Policies and Procedures	Review and update security policies and procedures at least annually.	Google provides audits assertions using industry accepted formats such as ISAE 3402, SOC 2/3 and ISO 27001. Google makes its SOC 2/3 report and ISO 27001 certificate available to customers. Google's security teams are committed to a strong perimeter and dedicated staff are responsible for the safety and security of Google's network infrastructure. Google conducts rigorous internal continuous testing of our network perimeter through various types of penetration exercises. In addition, Google coordinates external 3rd party penetration testing using qualified and certified penetration testers. Google conducts rigorous internal continuous testing of our application surface through various types of penetration exercises. In addition, Google coordinates external 3rd party penetration testing using qualified and certified penetration testers.	· Incorporate the following factors into the annual managerial review of security policies and procedures: o Recent security trends o Feedback from company personnel o New threats and vulnerabilities o Recommendations from regulatory agencies (i.e., FTC, etc.) o Previous security incidents	AAC-01 AAC-02

			Google maintains an internal audit program consistent with industry best practices and regulatory requirements. Google is committed to maintaining a program where independent verification of security, privacy and compliance controls are regularly reviewed. 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 27001 ISO 27017 / 27018 PCI-DSS HIPAA Google Security Policy prohibits sharing this information but customers may conduct their own testing on our products and services. Google publishes and makes available its ISO 27001, 27017, 27018 and SOC3 reports online. Detailed information of some confidential reports can be obtained under NDA. 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.		
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,	Google provides Google-specific security training. The training is administered online and completion tracked. Completion is required annually. 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. Completion of the training is required by our personnel policies. Google provides Google-specific security training. The training is administered online and	· 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	HRS-03 HRS-09

		and/or client requirements.	completion tracked. Completion is required annually. This is primarily a customer responsibility as they own their data. Google personnel are trained on the Data Security policy including procedures for handling customer data.	policies, procedures, and client requirements for all company personnel and third party workers	
MS-4.3	Policies and Procedures	Develop and regularly update an awareness program about security policies and procedures and train company personnel and third party workers upon hire and annually thereafter on those security policies and procedures, addressing the following areas at a minimum: · IT security policies and procedures · Content/asset security and handling in general and client-specific requirements · Security incident reporting and escalation · Disciplinary policy · Encryption and key management for all individuals who handle encrypted content	Google provides Google-specific security training. The training is administered online and completion tracked. Completion is required annually. This is primarily a customer responsibility as they own their data. Google personnel are trained on the Data Security policy including procedures for handling customer data.	· 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,	HRS-09

		· Asset disposal and destruction processes		production) to mitigate piracy issues · Consider recording training sessions and making recordings available for reference	
MS-5.0	Incident Response	Establish a formal incident response plan that describes actions to be taken when a security incident is detected and reported.	Google operates a global network of data centers to reduce risks from geographical disruptions. The link below includes the locations of our data centers: http://www.google.com/about/datacenters/inside/locations/ 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. Google maintains incident response procedures to help ensure prompt notification and investigation of incidents. Google has a 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. Testing of	· Consider including the following sections in the incident response plan: o Definition of incident o Notification of security team o Escalation to management o Analysis of impact and priority o Containment of impact o Eradication and recovery o Key contact information, including client studio contact information o Notification of affected business partners and clients o Notification of law enforcement o Report of details of incident · Reference NIST SP800-61 Revision 2 on Computer Security Incident Handling	BCR-01 SEF-01 SEF-02

			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. 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. https://cloud.google.com/terms/ Google performs annual testing of its emergency response processes.		
MS-5.1		Identify the security incident response team who will be responsible for detecting, analyzing, and remediating security incidents.	Google maintains automated log collection and analysis tools that collect and correlate log information from various sources. Google maintains automated log collection and analysis tools that support the investigation of incidents not caused by the tenant.	· Include representatives from different business functions in order to address security incidents of all types; consider the following: o Management o Physical security o Information security o Network team o Human resources o Legal · Provide training so that members of the incident response team understand their roles and responsibilities in handling incidents	SEF-03
MS-5.2	Incident Response	Establish a security incident reporting process for individuals to report detected incidents to the	Google maintains automated log collection and analysis tools that collect and correlate log information from various sources. Google maintains automated log collection and analysis tools that support the investigation of incidents not caused by the tenant.	· Consider implementing an anonymous hotline or website that can be used to report	SEF-03

		security incident response team.		inappropriate and/or suspicious activity · Consider implementing a group email address for reporting incidents that would inform all members of the incident response team · Consider leveraging the MPAA tips hotline for anonymous tips on suspicious activity – please refer to the 24-hour tip hotline contact information in Appendix H	
MS-5.3		Communicate incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client assets), and conduct a post-mortem meeting with management and client.	Google maintains automated log collection and analysis tools that collect and correlate log information from various sources. Google maintains automated log collection and analysis tools that support the investigation of incidents not caused by the tenant. Individual customers get notified should an incident impact their data. Google communicates outage information through our status dashboards: For Cloud Platform: https://status.cloud.google.com/ For Gsuite: https://www.google.com/appsstatus#hl=en&v=status	· 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	SEF-03 STA-02

				the corrective action plan, to affected clients	
MS-6.0	Business Continuity & Disaster Recovery	Establish a formal plan that describes actions to be taken to ensure business continuity.	Google operates a global network of data centers to reduce risks from geographical disruptions. The link below includes the locations of our data centers: http://www.google.com/about/datacenters/inside/locations/ 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 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. Due to the dynamic and sensitive nature of this information, Google does not share this information with tenants. 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. Engineering teams maintain procedures to facilitate the rapid reconstitution of services. Google anticipates physical threats to its datacenters and has implemented countermeasures to prevent or limit the impact from these threads. The video below provides an overview of our countermeasures: https://www.youtube.com/watch?v=cLory3qLoY8c' Google has implemented redundancies and safeguards in its datacenters to minimize the impact of service outages. Customers need to manage this by leveraging the features of our storage services. Please	· Consider including the following sections in the business continuity plan: o Threats to critical assets and content, including loss of power and telecommunications, systems failure, natural disasters etc. o Detailed information system, content and metadata backup procedures and information system documentation, including configuration of critical WAN and LAN / Internal Network devices o Encryption of backups (minimum of AES-128 bit encryption) o Backup power supply to support at least 15 minutes for the CCTV system, alarm and critical information systems, including software to perform a safe shutdown of critical systems o Consider use of an off-site backup location o Notification of security team o Escalation to management o Analysis of impact and priority o Containment of impact	BCR-01 BCR-02 BCR-03 BCR-04 BCR-05 BCR-08 BCR-11

			see the product documentation for specifics: https://cloud.google.com/docs/storing-your-data Customers are primarily responsible for legal requests. Google will assist customers where necessary. Google's process for handling law enforcement requests is detailed here: http://www.google.com/transparencyreport/userdatarequests/legalprocess/ 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. However, 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.	o Priorities for recovery and detailed recovery procedures, including manual workarounds and configuration details of restored systems o Key contact information o Notification of affected business partners and clients o Testing of business continuity and disaster recovery processes at least annually	
MS-6.1		Identify the business continuity team who will be responsible for detecting, analyzing and remediating continuity incidents.	Engineering teams maintain playbooks to facilitate the rapid reconstitution of services.	· Include defined roles and responsibilities · Provide training so that members of the business continuity team understand their roles and responsibilities	BCR-10
MS-7.0	Change Control & Configuration Management	Establish policies and procedures to ensure new data, applications, network, and systems components have been pre-approved by business leadership.	The authorization to provision additional processing capacity is obtained through budget approvals and managed through internal SLAs as part of an effective resource economy. https://cloud.google.com/docs/ https://gsuite.google.com/learning-center/ 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	· Include documentation that describes installation, configuration and use of devices, services and features, and update documentation as needed · Document policies and procedures for dealing with known issues	CCC-01 CCC-03 CCC-04 CCC-05

			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. Please see: http://www.google.com/about/appsecurity/reward-program/ 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. Google uses automated configuration management tools, software release tools and	· Include policies and procedures for reporting bugs and security vulnerabilities · Restrict and monitor the installation of unauthorized hardware or software · Manage risks associated with changes to data, applications, network infrastructure and systems · Document and retain all change requests, testing results and management approvals	

			mobile device management software to restrict and monitor the installation of unauthorized software. 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 whom 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.		
MS-8.0	Workflow	Document workflows tracking content and authorization checkpoints. Include the following processes for both physical and digital content: · Delivery (receipt/return) · Ingest · Movement · Storage · Removal/destruction		· 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	
MS-8.1		Update the workflow when there are changes to the process, and review the workflow process at least annually		· Follow the content workflow and implemented controls for each process in order to determine areas of vulnerability	

		to identify changes.			
MS-9.0	Segregation of Duties	Segregate duties within the content workflow. Implement and document compensating controls where segregation is not practical.	Google restricts access based on need-to-know and job functions. Google maintains automated log collection and analysis tools. Google maintains automated log collection and analysis tools. Multi-factor authentication is required for any connections to our production environment. Google maintains an automated access revocation process that include account locking and revocation of certificates and role assignment. Google logs all changes in user permissions with the date and time of such changes. Google's production environment is segregated from our corporate environment. Google provides (under a specific NDA) customers with a SOC 2/3 report that includes testing of Google's access controls. Details are documented here: https://cloud.google.com/security/whitepaper 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. Google restricts access based on need-to-know and job functions. Google maintains automated log collection and analysis tools.	· Document roles and responsibilities to eliminate an overlap of role-based job functions such as: o Vault and server/machine room personnel o Shipping and receiving personnel o Asset movement within facility (e.g., runners) from vault and content/production area o Digital asset folder access (e.g., data wrangler sets up access for producer) o 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: o Monitor the activity of company personnel and/or third party workers o Retain and review audit logs · Implement physical segregation	IAM-01 IAM-02 IAM-03 IAM-05 IAM-06

				· Enforce management supervision	
MS-10.0	Background Checks	Perform background screening checks on all company personnel and third party workers.	Google conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.	· 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	HRS-02
MS-11.0	Confidentiality Agreements	Require all company personnel to sign a confidentiality agreement (e.g., non-disclosure) upon hire and annually thereafter, that includes requirements for handling and	Google reviews NDA and confidentiality documents as needed.	· 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	HRS-06

		protecting content.		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	
MS-11.1		Require all company personnel to return all content and client information in their possession upon termination of their employment or contract.	Google's security incident response process includes involvement of our privacy team. Customers are notified when an events impacts their data. Google's privacy policy is informed by industry standards and tailored to Google's unique operation environment.		HRS-01
MS-12.0	Third Party Use and Screening	Require all third party workers (e.g., freelancers) who handle content to sign confidentiality agreements (e.g., non-disclosure) upon engagement.	Google reviews NDA and confidentiality documents as needed. Google provides Google-specific security training. The training is administered online and completion tracked. Completion is required annually. 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. Completion of the training is required by our personnel policies.	· 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	HRS-06 HRS-03

				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	
MS-12.1		Require all third party workers to return all content and client information in their possession upon termination of their contract.	Google's security incident response process includes involvement of our privacy team. Customers are notified when an events impacts their data. Google's privacy policy is informed by industry standards and tailored to Google's unique operation environment.		HRS-01
MS-12.2		Include security requirements in third party contracts.	Google permits customers to conduct their own vulnerability scans and penetration tests. In addition, Google maintains a robust bug bounty program and encourages input from the security community. For details see: http://www.google.com/about/appsecurity/reward-program/ Google retains a 3rd party to conduct periodic penetration tests.	· Require third party workers to comply with the security requirements specified in third party contracts and client requirements · Include a right to audit clause for activities that involve sensitive content · Implement a process to monitor for compliance with security requirements	STA-09
MS-12.3		Implement a process to reclaim content when terminating relationships.	Google's security incident response process includes involvement of our privacy team. Customers are notified when an events impacts their data. Google's privacy policy is informed by industry standards and tailored to Google's unique operation environment.	· Ensure all content on third party equipment is transferred to the organization and securely erased from the equipment	HRS-01
MS-12.4	Third Party Use and Screening	Require third party workers to be bonded and insured where		· Require third party workers to show proof of insurance and keep a record of their	

		appropriate (e.g., courier service).		insurance provider and policy number · Require third party insurance to meet a certain level of coverage · Require annual update of information when contracts are renewed	
MS-12.5		Restrict third party access to content/production areas unless required for their job function.	Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system 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 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. Customers can choose data location when they initiate project set up. This is covered by our service specific terms: https://cloud.google.com/terms/service-terms 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	· Ensure that third party workers are not given electronic access to areas housing content · Escort third party workers (e.g., cleaning crews) when access to restricted areas (e.g., vault) is required	DCS-02 DCS-07 DCS-09 IAM-07

			authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request 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. Google automatically replicates to and serves data from multiple data centers to provide seamless access to end-users should a datacenter not be available. Google has designed redundancies in its system to help prevent service interruptions in the event of failure of in Google or a provider operated infrastructure. We have redundancy for critical services such as telecommunication links. Google runs and maintains its own infrastructure and does not depend on external services. Due to both the dynamic and sensitive nature of this information, Google does not provide this information externally. However, macro service availability is visible below, and the regional coverage and guides on deploying highly available services is also available. https://status.cloud.google.com/ https://cloud.google.com/about/locations/ https://cloud.google.com/docs/geography-and-regions A tenant can contact support 24/7 to raise issues. Google Cloud platform provides a managed load balancing and failover capability to customers.		

			https://cloud.google.com/compute/docs/load-balancing/ Our business continuity program is verified as part of our SOC 2/3 audit report.		
MS-12.6		Notify clients if subcontractors are used to handle content or work is offloaded to another company.	Customers are responsible for configuring the access by their uses to the service. For Google personnel, authorization is required prior to access being granted. Customers are responsible for configuring the access by their users to the service. For Google personnel, authorization is required prior to access being granted.	· Require written client sign-off/approval · Require subcontractors to go through standard due diligence activities · Work offloaded to another company must be reported to the MPAA member studios, and the MPAA Vendor Questionnaire must be completed and provided to the member studios for their due diligence.	IAM-09
PS-1.0	Entry/Exit Points	Secure all entry/exit points of the facility at all times, including loading dock doors and windows.	Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system 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 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.	· 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	DCS-02 DCS-07

			Customers can choose data location when they initiate project set up. This is covered by our service specific terms: https://cloud.google.com/terms/service-terms		
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).	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 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.	· 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	DCS-09
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	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.		DCS-06

		· Logging and monitoring of all entrances and exits within facility · All tenants within the facility must be reported to client prior to engagement			
PS-2.0	Visitor Entry/Exit	Maintain a detailed visitors' log and include the following: · Name · Company · Time in/time out · Person/people visited · Signature of visitor · Badge number assigned	Google maintains a central identity and authorization management system.	· 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	IAM-04
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 centralized controlled and monitored system.	· 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	

PS-2.2		Do not provide visitors with key card access to content/production areas.	Visitors are not given card access		
PS-2.3		Require visitors to be escorted by authorized employees while on-site, or in content/production areas.	All visitors must be escorted at all times		
PS-3.0	Identification	Provide company personnel and long-term third party workers (e.g., janitorial) with a photo identification badge that is required to be visible at all times.	All employees and contractors are given specially printed photo ID badges and must wear them visibly at all times	· 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	
PS-4.0	Perimeter Security	Implement perimeter security controls that address risks that the facility may be exposed to as identified by the organization's risk assessment.	Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system 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 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.	· Implement security controls based upon the location and layout of the facility, such as: o 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 o Securing and enclosing, as necessary, common external areas such as smoking areas and open balconies o Sufficient external camera coverage around common exterior areas (e.g., smoking areas), as well as parking o Being cognizant of the overuse of company signage that could create targeting o Using alarms around the perimeter, as necessary	DCS-02
PS-4.1		Place security guards at perimeter entrances and non- emergency entry/exit points.	Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system 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 restricted based on an individual's		DCS-02

			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.		
PS-4.2	Perimeter Security	Implement a daily security patrol process with a randomized schedule and document the patrol results in a log.	Physcial security personal patrol all Google work areas and datacenters.	· Require security guards to patrol both interior and exterior areas · Include a review of emergency exits, including verification of seals · Consider using a guard tour patrol system to track patrolling (e.g., Checkpoint) and verify locks	
PS-4.3		Lock perimeter gates at all times.	Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system 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 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	· 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 proper paperwork · Require visitor vehicles to present identification and ensure that all visitors have been pre-authorized to enter the premises	DCS-02

			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.		
PS-5.0	Alarms	Install a centralized, audible alarm system that covers all entry/exit points (including emergency exits), windows, loading docks, fire escapes, and restricted areas (e.g., vault, server/machine room, etc.).	Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system 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 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. Customers can choose data location when they initiate project set up. This is covered by our service specific terms: https://cloud.google.com/terms/service-terms	· Place alarms at every entrance to alert security personnel upon unauthorized entry to the facility · Enable the alarm when facility is unsupervised	DCS-02 DCS-07
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,	Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system 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 restricted based on an individual's job responsibilities. The fire doors at the data centers are alarmed and can only be opened	· Ensure the alarm system covers storage areas and vaults (e.g., through motion sensors) after normal business hours, as an added layer of security	

		producer, head of editorial, incident response team, etc.).	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.		
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 pre-determined period of time (e.g., 60 seconds).	Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system 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 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.	· Configure access-controlled doors to trigger alarms and alert security personnel when doors have been propped open for an extended period of time	
PS-5.3	Alarms	Configure alarms to provide escalation notifications directly to the personnel in charge of security and other personnel (e.g., project managers, producer, head of	Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system 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 restricted based on an individual's	· 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	

		editorial, incident response team, etc.).	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.	notification upon breach · Implement procedures for notification on weekends and after business hours	
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.	Google maintains a central identity and authorization management system.	· Use unique alarm codes to track which security personnel was responsible for arming/disarming the alarm · Update assigned alarm codes at an interval approved by management in order to reduce risk involved with sharing and losing codes	IAM-04
PS-5.5		Review the list of users who can arm and disarm alarm systems quarterly, or upon change of personnel.	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 maintains an automated access revocation process that include account locking and revocation of certificates and role assignment. Google logs all changes in user permissions with the date and time of such changes. Google provides (under a specific NDA) customers with a SOC 2/3 report that includes testing of Google's access controls. Details are documented here: https://cloud.google.com/security/whitepaper	· Remove users who have left the company or have changed job roles · Deactivate the alarm codes that were assigned to removed users	IAM-10 IAM-02 IAM-05

PS-5.6		Test the alarm system quarterly.	Google performs periodic network vulnerability scans using commercial tools. Google performs periodic application-layer vulnerability scans using commercial and proprietary tools. Google performs periodic 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 monitor 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 guides. https://cloud.google.com/security/whitepaper https://cloud.google.com/terms/	· Simulate a breach in physical security and ensure the following: o Alarm system detects the breach o Security personnel are alerted o Security personnel respond in a timely manner according to procedures	TVM-02
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.			
PS-6.0	Authorization	Document and implement a process to manage facility access and keep records of any changes to access rights.	Google maintains an automated access revocation process that include account locking and revocation of certificates and role assignment. Google logs all changes in user permissions with the date and time of such changes. Google provides (under a specific NDA) customers with a SOC 2/3 report that includes testing of Google's access controls. Details are documented here: https://cloud.google.com/security/whitepaper	· 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	IAM-02 IAM-05

				supervisor to request facility access for company personnel and/or third party workers · 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. https://cloud.google.com/solutions/devtest/ Google segregates its production environment from its corporate environment.		IVS-08
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.	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.	· 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	IAM-10
PS-7.0	Electronic Access Control	Implement electronic access throughout the facility to cover all entry/exit points and all areas where content is stored, transmitted, or processed.	Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system 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 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	· 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	DCS-02

			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.	· See Logging and Monitoring PS-10.0 · Review the times when electronic access is not required for common areas (e.g., public elevators)	
PS-7.1	Electronic Access Control	Restrict electronic access system administration to appropriate personnel.	Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system 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 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.	· 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	
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	Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system 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 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	· Limit access to the locked cabinet to the keycard / electronic access device system administration team · Require sign-out for inventory removal	

		devices (e.g., keycards, key fobs) in a locked cabinet and ensure these remain disabled prior to being assigned to personnel.	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.		
PS-7.3		Disable lost electronic access devices (e.g., keycards, key fobs) in the system before issuing a new electronic access device.	Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system 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 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.	· 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	
PS-7.4		Issue third party access electronic access devices with a set expiration date (e.g. 90 days) based on an approved timeframe.	Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system 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 restricted based on an individual's job responsibilities. The fire doors at the data	· 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	

			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.	· Assign third party electronic access devices on a need-to-know basis	
PS-8.0	Keys	Limit the distribution of master keys and / or keys to restricted areas to authorized personnel only (e.g., owner, facilities management).	Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system 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 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.	· 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	
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.	Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system 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	· Maintain records to track the following information: o Company personnel in possession of each master key o Time of check-out/check-in o Reason for check-out	

			centers is 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.	· 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.	Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system 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 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.	· Use high-security keys (cylinders) that offer a greater degree of resistance to any two or more of the following: o Picking o Impressioning o Key duplication o Drilling o Other forms of forcible entry	
PS-8.3		Inventory master keys and keys to restricted areas, including facility entry/exit points, quarterly.	Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system 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	· Identify, investigate, and address any missing keys (lost/stolen) · Review logs to determine who last checked out a key that	

			investigated as appropriate. Authorized access throughout the business operations and data centers is 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.	cannot be accounted for · Change the locks when missing master keys or keys to restricted areas cannot be accounted for	
PS-8.4		Obtain all keys from terminated employees/third-parties or those who no longer need the access.	Google's security incident response process includes involvement of our privacy team. Customers are notified when an events impacts their data. Google's privacy policy is informed by industry standards and tailored to Google's unique operation environment.		HRS-01
PS-8.5	Keys	Implement electronic access control or rekey entire facility when master or sub-master keys are lost or missing.	Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system 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 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.		
PS-9.0	Cameras	Install a CCTV system that records all facility entry/exit points and restricted areas (e.g. server/machine room, etc.).	Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system 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 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.	· Camera cables and wiring should be discretely hidden from view and not within reasonable reach · Facility should not assume that CCTV provided by the building is adequate · Place cameras at every entrance to the facility · Ensure the cameras cover storage areas and vaults	DCS-02
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.	Google anticipates physical threats to its datacenters and has implemented countermeasures to prevent or limit the impact from these threads. The video below provides an overview of our countermeasures: https://www.youtube.com/watch?v=cLory3qLoY8c'	· Review camera positioning to ensure an unobstructed view of all entry/exit points and other sensitive areas · Accommodate for cameras in dark areas (e.g., low-light or infrared cameras, motion-detecting lights) · Review image quality to ensure that lighting is adequate and that faces are distinguishable · Review frame rate to ensure that activity is adequately recorded	

				· Position cameras to avoid capturing content on display · Record with sufficient resolution to be able to identify facial features · Record at a minimum rate of 7 frames per second	
PS-9.2		Restrict physical and logical access to the CCTV console and to CCTV equipment (e.g., DVRs) to personnel responsible for administering/monitoring the system.	Google restricts access based on need-to-know and job functions. Google maintains automated log collection and analysis tools. 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. Google provides (under a specific NDA) customers with a SOC 2/3 report that includes testing of Google's access controls. Details are documented here: https://cloud.google.com/security/whitepaper	· Place CCTV 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 CCTV systems is restricted to authorized personnel and that strong account management controls are in place (e.g., password complexity, individual user login, logging and monitoring)	IAM-01 IAM-04 IAM-05
PS-9.3	Cameras	Ensure that camera footage includes an accurate date and time-stamp and retain CCTV surveillance footage and electronic access logs for at least 90 days, or the maximum time allowed by law, in a secure location.	Google anticipates physical threats to its datacenters and has implemented countermeasures to prevent or limit the impact from these threads. The video below provides an overview of our countermeasures: https://www.youtube.com/watch?v=cLory3qLoY8c'	· 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 CCTV 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.	Google anticipates physical threats to its datacenters and has implemented countermeasures to prevent or limit the impact from these threads. The video below provides an overview of our countermeasures: https://www.youtube.com/watch?v=cLory3qLoY8c'	· Incorporate the incident response process for handling security incidents · Consider adding a surveillance monitor at the reception desk or in the IT office	
PS-10.0	Logging and Monitoring	Log and review electronic access to restricted areas for suspicious events, at least weekly.	Google anticipates physical threats to its datacenters and has implemented countermeasures to prevent or limit the impact from these threads. The video below provides an overview of our countermeasures: https://www.youtube.com/watch?v=cLory3qLoY8c'	· 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:	

				o Repeated failed access attempts o Unusual time-of-day access o Successive door access across multiple zones	
PS-10.1	Logging and Monitoring	Log and review electronic access, at least daily, for the following areas: · Masters/stampers vault · Pre-mastering · Server/machine room · Scrap room · High-security cages	Google anticipates physical threats to its datacenters and has implemented countermeasures to prevent or limit the impact from these threads. The video below provides an overview of our countermeasures: https://www.youtube.com/watch?v=cLory3qLoY8c'	· Identify and document events that are considered unusual · 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.	Google machine configuration changes are continuously monitored when online. Google Cloud platform provides the ability to log and monitor the health of virtual instances using variety of tools : https://console.developers.google.com https://cloud.google.com/docs/	· 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	IVS-02?
PS-10.3		Maintain an ongoing log of all confirmed electronic access incidents and include documentation of any follow-up activities that were taken.	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.	· Leverage the incident response reporting form to document confirmed keycard / electronic access device incidents · Review all recent keycard / electronic access device incidents periodically and	SEF-05

				perform root-cause analysis to identify vulnerabilities and appropriate fixes	
PS-11.0	Searches	Establish a policy, as permitted by local laws, which allows security to randomly search persons, bags, packages, and personal items for client content.	Google anticipates physical threats to its datacenters and has implemented countermeasures to prevent or limit the impact from these threads. The video below provides an overview of our countermeasures: https://www.youtube.com/watch?v=cLory3qLoY8c'	· Communicate policies regarding search to all company personnel and third party workers · Conduct searches periodically of company personnel and third party workers to validate policy	
PS-11.1	Searches	Implement an exit search process that is applicable to all facility personnel and visitors, including: · Removal of all outer coats, hats, and belts for inspection · Removal of all pocket contents · Performance of a self pat-down with the supervision of security · Thorough inspection of all bags · Inspection of laptops' CD/DVD tray · Scanning of individuals with a handheld metal detector used within three inches of the individual searched	Google anticipates physical threats to its datacenters and has implemented countermeasures to prevent or limit the impact from these threads. The video below provides an overview of our countermeasures: https://www.youtube.com/watch?v=cLory3qLoY8c'	· 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	

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.	Google anticipates physical threats to its datacenters and has implemented countermeasures to prevent or limit the impact from these threads. The video below provides an overview of our countermeasures: https://www.youtube.com/watch?v=cLory3qLoY8c'	· 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	
PS-11.3		Enforce the use of transparent plastic bags and food containers for any food brought into production areas.	Google anticipates physical threats to its datacenters and has implemented countermeasures to prevent or limit the impact from these threads. The video below provides an overview of our countermeasures: https://www.youtube.com/watch?v=cLory3qLoY8c'	· Consider designating an area for eating food outside of the production area	
PS-11.4		Implement a dress code policy that prohibits the use of oversized clothing (e.g., baggy pants, oversized hooded sweatshirts).	Google anticipates physical threats to its datacenters and has implemented countermeasures to prevent or limit the impact from these threads. The video below provides an overview of our countermeasures: https://www.youtube.com/watch?v=cLory3qLoY8c'		
PS-11.5		Use numbered tamper-evident stickers/holograms to identify authorized devices that can be taken in and out of the facility.	Google anticipates physical threats to its datacenters and has implemented countermeasures to prevent or limit the impact from these threads. The video below provides an overview of our countermeasures: https://www.youtube.com/watch?v=cLory3qLoY8c'		

PS-11.6	Searches	Implement a process to test the exit search procedure.	Google provides audits assertions using industry accepted formats such as ISAE 3402, SOC 2/3 and ISO 27001.	· 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	AAC-01
PS-11.7		Perform a random vehicle search process when exiting the facility parking lot.	Google anticipates physical threats to its datacenters and has implemented countermeasures to prevent or limit the impact from these threads. The video below provides an overview of our countermeasures: https://www.youtube.com/watch?v=cLory3qLoY8c'		
PS-11.8		Segregate replication lines that process highly sensitive content and perform searches upon exiting segregated areas.	Google does not depend on supply-chain partners for data quality with respect to delivering the Google Cloud Platform service. 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. Customers can provision separate domains or organizations with a domain for testing purposes. Google provides solution papers and reference Development and Test environments. https://cloud.google.com/solutions/devtest/ Google segregates its production environment from its corporate environment.		STA-01? IVS-08?
PS-11.9		Implement additional controls to monitor security guards activity.	Google anticipates physical threats to its datacenters and has implemented countermeasures to prevent or limit the impact from these threads. The video below provides an overview of our countermeasures: https://www.youtube.com/watch?v=cLory3qLoY8c'	· 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)	

PS-12.0	Inventory Tracking	Implement a content asset management system to provide detailed tracking of physical assets (i.e., received from client created at the facility).	Google's Device Policy Manager enforces Google's mobile policy except when access is solely to Apps services and through a browser. Google uses certificates and ACLs to achieve authentication integrity. 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 GCP users, the locality of data is for the most part customer controlled and is described here: https://cloud.google.com/docs/geography-and-regions All devices must register through the Google Device Policy Manager unless browser-only access is used.	· 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	MOS-10 DCS-03 DCS-04 MOS-09
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.	Google's Device Policy Manager enforces Google's mobile policy except when access is solely to Apps services and through a browser.	· 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	MOS-10
PS-12.2		Retain asset movement	Google anticipates physical threats to its datacenters and has implemented	· Store physical or digital logs for all asset	

		transaction logs for at least one year.	countermeasures to prevent or limit the impact from these threads. The video below provides an overview of our countermeasures: https://www.youtube.com/watch?v=cLory3qLoY8c'	movements; logs should include: o Barcode or unique ID of asset that was checked-in/checked-out o Time and date of check-in/check-out o Name and unique ID of the individual who checked out an asset o Reason for checkout o Location of asset	
PS-12.3	Inventory Tracking	Review logs from content asset management system at least weekly and investigate anomalies.	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 ISO27002. Google maintains an automated log collection and analysis tool to review and analyse log events.	· 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	IVS-01
PS-12.4		Use studio film title aliases when applicable on physical assets and in asset tracking systems.	NA	· Consider removing the studio name on physical assets, when appropriate	
PS-12.5		Implement and review a daily aging report to identify highly sensitive assets that are checked out from the vault	Google anticipates physical threats to its datacenters and has implemented countermeasures to prevent or limit the impact from these threads. The video below provides an overview of our countermeasures: https://www.youtube.com/watch?v=cLory3qLoY8c'	· Perform daily aging reports either manually or through an asset management system · Investigate all exceptions	

		and not checked back in.			
PS-12.6		Lock up and log assets that are delayed or returned if shipments could not be delivered on time.	Google anticipates physical threats to its datacenters and has implemented countermeasures to prevent or limit the impact from these threads. The video below provides an overview of our countermeasures: https://www.youtube.com/watch?v=cLory3qLoY8c'	· 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	
PS-13.0	Inventory Counts	Perform a quarterly inventory count of each client's asset(s), reconcile against asset management records, and immediately communicate variances to clients.	Google maintains assets inventories and assigns ownership for managing its critical resources. Google maintains a list of Sub-Processors: https://www.google.com/intx/en/work/apps/terms/subprocessors.html		DCS-01
PS-13.1		Segregate duties between the vault staff and individuals who are responsible for performing inventory counts.	Google does not depend on supply-chain partners for data quality with respect to delivering the Google Cloud Platform service. 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.	· Assign non-vault staff personnel to do random checks of count results	STA-01
PS-14.0	Blank Media/ Raw Stock Tracking	Tag (e.g., barcode, assign unique identifier) blank stock/raw stock per unit when received.	Google does not depend on supply-chain partners for data quality with respect to delivering the Google Cloud Platform service. 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.	· Do not allow blank or raw media stock in secured production areas unless it is required for production purposes	STA-01?
PS-14.1		Establish a process to track consumption of raw materials (e.g.,	Google does not depend on supply-chain partners for data quality with respect to delivering the Google Cloud Platform service. Google employs a vendor management process that includes contractual requirements	· Reconcile existing raw stock with work orders to identify variances in inventory	STA-01?

		polycarbonate) monthly.	to adhere to Google's security policies and onsite inspections, as needed, to confirm compliance.	· Establish a variance threshold that trippers the incident response process when exceeded · Consider the execution of physical counts of raw stock as part of the monthly tracking process	
PS-14.2		Store blank media/raw stock in a secured location.	Google does not depend on supply-chain partners for data quality with respect to delivering the Google Cloud Platform service. 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.	· 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	STA-01?
PS-15.0	Client Assets	Restrict access to finished client assets to personnel responsible for tracking and managing assets.	Google maintains an automated access revocation process that include account locking and revocation of certificates and role assignment. Google logs all changes in user permissions with the date and time of such changes. Google does not depend on supply-chain partners for data quality with respect to delivering the Google Cloud Platform service. 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.	· 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	IAM-02 STA-01
PS-15.1		Store client assets in a restricted and secure area (e.g., vault, safe, or other secure storage location).	Google anticipates physical threats to its datacenters and has implemented countermeasures to prevent or limit the impact from these threads. The video below provides an overview of our countermeasures:	· Implement an additional safe or high-security cage within the vault for highly sensitive titles	

			https://www.youtube.com/watch?v=cLory3qLoY8c'	· Secure the safe to the wall or floor by bolting it to the room structure	
PS-15.2		Require two company personnel with separate access cards to unlock highly sensitive areas (e.g., safe, high-security cage) after-hours.	Google maintains an automated access revocation process that include account locking and revocation of certificates and role assignment. Google logs all changes in user permissions with the date and time of such changes.		IAM-02
PS-15.3	Client Assets	Use a locked fireproof safe to store undelivered packages that are kept at the facility overnight.	Google anticipates physical threats to its datacenters and has implemented countermeasures to prevent or limit the impact from these threads. The video below provides an overview of our countermeasures: https://www.youtube.com/watch?v=cLory3qLoY8c'	· Secure the safe by bolting it to an immovable surface (e.g., floor, wall)	BCR-05
PS-15.4		Implement a dedicated, secure area (e.g., security cage, secure room) for the storage of undelivered screeners that is locked, access-controlled, and monitored with surveillance cameras and/or security guards.	Customers can choose data location when they initiate project set up. This is covered by our service specific terms: https://cloud.google.com/terms/service-terms	· 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	DCS-07
PS-16.0	Disposals	Require that rejected, damaged, and obsolete stock containing client assets are erased, degaussed, shredded, or physically	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 appropriate operations manager before release.	· 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	DCS-05

		destroyed before disposal.		· Consider referencing U.S. Department of Defense 5220.22-M for digital shredding and wiping standards (see appendix G)	
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.	Customers can choose data location when they initiate project set up. This is covered by our service specific terms: https://cloud.google.com/terms/service-terms	· 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	DCS-07
PS-16.2		Maintain a log of asset disposal for at least 12 months.	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 appropriate operations manager before release.	· Integrate the logging of asset disposal into the asset management process · Include a final disposal record for disposed assets in disposal logs	
PS-16.3	Disposals	Destruction must be performed on site. On site destruction must be supervised and signed off by two company personnel. If a third party destruction company is engaged, destruction must be supervised and signed off by two company personnel and certificates of	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 appropriate operations manager before release.	· Consider requiring the following information on the certificate of destruction: o Date of destruction o Description of the asset destroyed/disposed of o Method of destruction o Name of individual who destroyed the assets	DCS-05

		destruction must be retained.			
PS-16.4		Use automation to transfer rejected discs from replication machines directly into scrap bins (no machine operator handling).	Google provides (under a specific NDA) customers with a SOC 2/3 report that includes testing of Google's access controls. Details are documented here: https://cloud.google.com/security/whitepaper	· 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	IAM-05
PS-17.0	Shipping	Require the facility to generate a valid work/shipping order to authorize client asset shipments out of the facility.	Google does not depend on supply-chain partners for data quality with respect to delivering the Google Cloud Platform service. 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 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 GCP users, the locality of data is for the most part customer controlled and is described here: https://cloud.google.com/docs/geography-and-regions	· Include the following information on the work/shipping order: o Work/shipping order number o Name and company of individual who will pick up content o Time and date of pick up o Facility contact · Create a form for documenting outbound assets that are transported via uncommon methods	STA-01 DCS-04
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	Google does not depend on supply-chain partners for data quality with respect to delivering the Google Cloud Platform service. 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.	· Require recipient signature · Retain shipping logs for a minimum of 1 year	STA-01

		· Address of destination · Tracking number from courier · Reference to the corresponding work order			
PS-17.2		Secure client assets that are waiting to be picked up.	Google does not depend on supply-chain partners for data quality with respect to delivering the Google Cloud Platform service. 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.	· Lock all doors and windows to shipping and receiving areas when unattended · Assets must be locked up until handed off to the vendor/courier	STA-01
PS-17.3		Validate client assets leaving the facility against a valid work/shipping order.	Google does not depend on supply-chain partners for data quality with respect to delivering the Google Cloud Platform service. 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.	· 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	STA-01
PS-17.4	Shipping	Prohibit couriers and delivery personnel from entering content/production areas of the facility.	Google does not depend on supply-chain partners for data quality with respect to delivering the Google Cloud Platform service. 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 Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system that are linked to a system alarm. Access to perimeter doors, shipping and receiving, and other critical areas is logged, including	· Escort delivery personnel if access to content/production areas is necessary	STA-01 DCS-02

			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 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.		
PS-17.5		Document and retain a separate log for truck driver information.	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.	· Maintain a log of all truck drivers and include the following information: o Name o License tags for the tractor and trailer o Affiliated company o Time and date of pick up o Content handled	
PS-17.6		Observe and monitor the on-site packing and sealing of trailers prior to shipping.	Google does not depend on supply-chain partners for data quality with respect to delivering the Google Cloud Platform service. 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.	· Require security personnel to be present at all times while trailers are loaded and sealed	STA-01
PS-17.7		Record, monitor and review travel times, routes, and delivery times for shipments between facilities.	This doesn't apply to GCP operations	· 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	
PS-17.8		Prohibit the transfer of film elements other than for client studio approved purposes.	This doesn't apply to GCP operations		
PS-17.9		Ship prints for pre-theatrical screenings in segments (e.g., odd versus even reels).	This doesn't apply to GCP operations		
PS-18.0	Receiving	Inspect delivered client assets upon receipt and compare to shipping documents (e.g., packing slip, manifest log).	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.	· Identify and log any discrepancies (e.g., missing items, damaged media) · Report discrepancies to management, clients, and/or the sender immediately	
PS-18.1	Receiving	Maintain a receiving log to be filled out by designated personnel upon receipt of deliveries.	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.	· Record the following information: o Name and signature of courier/delivering entity o Name and signature of recipient o Time and date of receipt o Details of received asset	
PS-18.2		Perform the following actions immediately:	Google maintains assets inventories and assigns ownership for managing its critical resources. Google maintains a list of Sub-Processors:	· Store received assets that cannot be immediately tagged and vaulted in a secure	

		· 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)	https://www.google.com/intx/en/work/apps/terms/subprocessors.html	staging area (e.g., high-security cage)	
PS-18.3		Implement a secure method for receiving overnight deliveries.	Where applicable overnight deliveries will be secured.	· Ensure that schedules for expected items are only available to people who need to see them	
PS-19.0	Labeling	Prohibit the use of title information, including AKAs ("aliases"), on the outside of packages unless instructed otherwise by client.	All packages are security inspected and routed to proper people		
PS-20.0	Packaging	Ship all client assets in closed/sealed containers, and use locked containers depending on asset value, or if instructed by the client.	This doesn't apply to GCP operations		
PS-20.1		Implement at least one of the following controls: · Tamper-evident tape · Tamper-evident packaging	This doesn't apply to GCP operations	· 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)	

		· Tamper-evident seals (e.g., in the form of holograms) · Secure containers (e.g., Pelican case with a combination lock)			
PS-20.2	Packaging	Apply shrink wrapping to all shipments, and inspect packaging before final shipment to ensure that it is adequately wrapped.	This doesn't apply to GCP operations	· Apply shrink wrapping to individual assets (e.g., skids, pallets) or per spindle if bulk shipments are performed	
PS-21.0	Transport Vehicles	Lock automobiles and trucks at all times, and do not place packages in clear view.	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.	· Do not leave packages unattended	
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	Google maintains assets inventories and assigns ownership for managing its critical resources. Google maintains a list of Sub-Processors: https://www.google.com/intx/en/work/apps/terms/subprocessors.html	· Use vehicles equipped with GPS tracking systems for delivery of sensitive content and high-value assets	
PS-21.2		Apply numbered seals on cargo doors for shipments of highly sensitive titles.	This doesn't apply to GCP operations	· 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	
PS-21.3		Require security escorts to be used when delivering highly sensitive content to high-risk areas.	This doesn't apply to GCP operations	· Hire security personnel capable of protecting highly sensitive content from hijacking, mugging, and other scenarios that could result in content theft	
DS-1.0	Firewall/WAN/ Perimeter Security	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.	Customers can provision separate domains or organizations with a domain for testing purposes. Google provides solution papers and reference Development and Test environments. https://cloud.google.com/solutions/devtest/ Google segregates its production environment from its corporate environment. Google does not permit wireless access in the production environment. Google has established policies and procedures to manage in corporate wireless network perimeter. Google does not permit wireless access points in its production environment. Google has established strong encryption and authentication to its corporate wireless network. Google does not permit wireless access points in its production environment and periodically scans for rogue devices.	· 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	IVS-08 IVS-12

				· Consider including the following in the firewall configuration: o Anti-spoofing filters o Block non-routable IP addresses o Block internal addresses over external ports o Block UDP and ICMP echo requests o Block unused ports and services o Block unauthorized DNS zone transfers o Apply egress filtering, so outgoing traffic can only come from an internal address	
DS-1.1	Firewall/WAN/ Perimeter Security	Implement a process to review firewall Access Control Lists (ACLs) to confirm configuration settings are appropriate and required by the business every 6 months.	cloud.google.com/docs 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 in monitored continuously. Network ACLs are documented within configuration files with comments on purpose, as appropriate.	· 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 · Update ACLs accordingly	IVS-06
DS-1.2		Deny all protocols by default and enable only specific permitted secure protocols to access the WAN and firewall.	Google builds in own machines and deploys custom operating system images that only permit the necessary ports, protocols and services.	· Restrict all unencrypted communication protocols such as Telnet and FTP · Replace unencrypted protocols with encrypted versions	IVS-07
DS-1.3		Place externally accessible servers (e.g., web servers) within the DMZ.	Customers can provision separate domains or organizations with a domain for testing purposes. Google provides solution papers and reference Development and Test environments. https://cloud.google.com/solutions/devtest/	· Isolate servers in the DMZ to provide only one type of service per server (e.g., web server, etc.)	IVS-08

			Google segregates its production environment from its corporate environment.	· Implement ACLs to restrict access to the internal network from the DMZ	
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.	Google has a dedicated process tied to the SLDC for patching all network devices and equipment.	· 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	
DS-1.5	Firewall/WAN/ Perimeter Security	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.	Google builds in own machines and deploys custom operating system images that only permit the necessary ports, protocols and services.	· Consider the following hardening options: o Disable guest accounts and shares o Install anti-virus / anti-malware o Enable software firewalls o Remove unnecessary software o Uninstall/disable unneeded services o Require all users to run as restricted users o Use an ACL that restricts access to the device so that only authorized management systems may be used to connect using SNMP	IVS-07

				· Refer to the following security hardening standards for hardening network infrastructure devices: o NIST o SANS o NSA	
DS-1.6		Do not allow remote management of the firewall from any external interface(s).	All access to production systems are based on least privilege, requires two-factor authentication, and is logged.	· Instead use two-factor authentication and a VPN connection with advanced encryption standard (AES) at 128 bits or higher to carryout remote administration functions · Require individuals to provide two of the following for non-administrative remote access: o Information that the individual knows (e.g., username, password) o A unique physical item that the individual has (e.g., token, keycard, smartphone, certificate) o A unique physical quality/biometrics that is unique to the individual (e.g., fingerprint, retina)	IVS-11
DS-1.7	Firewall/WAN/Perimeter Security	Secure backups of network infrastructure/SAN/NAS devices and servers to a centrally secured server on the internal network.	Customers need to manage this by leveraging the features of our storage services. Please see the product documentation for specifics: https://cloud.google.com/docs/storing-your-data Customers are primarily responsible for legal requests. Google will assist customers where necessary. Google's process for handling law enforcement requests is detailed here: http://www.google.com/transparencyreport/userdatarequests/legalprocess/	· 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	BCR-11

			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. However, 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.	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	
DS-1.8		Perform quarterly vulnerability scans of all external IP ranges and hosts at least and remediate issues.	Google performs periodic network vulnerability scans using commercial tools. Google performs periodic application-layer vulnerability scans using commercial and proprietary tools. Google performs periodic 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 monitor 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 guides. https://cloud.google.com/security/whitepaper https://cloud.google.com/terms/	· Remediate critical issues that provide unauthorized access to content 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	TVM-02
DS-1.9		Perform annual penetration testing of all external IP ranges and hosts at least	Google performs periodic network vulnerability scans using commercial tools. Google performs periodic application-layer vulnerability scans using commercial and proprietary tools.	· Remediate critical issues that provide unauthorized access to content in a timely manner	TVM-02

		and remediate issues.	Google performs periodic 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 monitor 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 guides. https://cloud.google.com/security/whitepaper https://cloud.google.com/terms/	· Ensure that tools used for scanning/testing accommodate virtualization technologies, if being used · Consider having this performed by an independent third-party	
DS-1.10		Secure any point to point connections by using dedicated, private connections and by using encryption.	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 (currently in Beta) which allows customers to supply their own encryption keys via API. Google maintains documentation on its key management process. Google maintains documentation on its key management process and provides controls to manage encryption keys through their lifecycle and protect against unauthorized use. Google uses a combination of open source and proprietary code to develop its encryption solutions We encrypt data at rest in Google Cloud Platform. Network packets are encrypted when they leave Google Compute Engine Instances. Google has a service (currently in Beta) which allows customers to supply their own encryption keys via API.	· Use advanced encryption standard (AES) at 128 bits or higher for encryption	EKM-02 EKM-03

			Google maintains internal documentation for the use of its internal proprietary key management service.		
DS-1.11		Implement a synchronized time service protocol (e.g., Network Time Protocol) to ensure all systems have a common time reference.	Google uses a synchronized time-service protocol to ensure all systems have a common time reference.	· Ensure systems have the correct and consistent time · Ensure time data is protected · Ensure time settings are received from industry-accepted time sources	IVS-03
DS-1.12	Firewall/WAN/ Perimeter Security	Establish, document and implement baseline security requirements for WAN network infrastructure devices and services.	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	· 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	CCC-03 GRM-01

			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. Please see: http://www.google.com/about/appsecurity/reward-program/ 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. 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. 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 platform. https://cloud.google.com/compute/docs/tutorials/building-images		
DS-2.0	Internet	Prohibit production network and all systems that process or store digital content from directly accessing the internet, including email. If a business case requires internet access from the production network or from systems that process or store	Customers can provision separate domains or organizations with a domain for testing purposes. Google provides solution papers and reference Development and Test environments. https://cloud.google.com/solutions/devtest/ Google segregates its production environment from its corporate environment.	· Handle exceptions using an Internet gateway system (e.g., Citrix, Terminal Services, VNC, etc.) with the following controls: o The system is tightly controlled where web browsing is the only function of the server o Access to restricted sites is prohibited, including web-based email sites, peer-to-peer, digital	IVS-08

		digital content, only approved methods are allowed via use of a remote hosted application / desktop session.		lockers, and other known malicious sites o Restrict content from being transferred to or from the system o Patch and update the system regularly with the latest virus definitions o Review system activity regularly o 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 · 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.	
DS-2.1	Internet	Implement email filtering software or appliances that block the following from non-production networks:	Customers can provision separate domains or organizations with a domain for testing purposes. Google provides solution papers and reference Development and Test environments. https://cloud.google.com/solutions/devtest/ Google segregates its production environment from its corporate environment.	· Identify restricted content types for email attachments and email message body · Implement an email filtering solution and configure based on restricted content types	IVS-08

		· Potential phishing emails · Prohibited file attachments (e.g., Visual Basic scripts, executables, etc.) · File size restrictions limited to 10 MB · Known domains that are sources of malware or viruses			
DS-2.2		Implement web filtering software or appliances that restrict access to websites known for peer-to-peer file trading, viruses, hacking or other malicious sites.	Google provides (under a specific NDA) customers with a SOC 2/3 report that includes testing of Google's access controls. Details are documented here: https://cloud.google.com/security/whitepaper	· Implement web-filtering/proxy server software to detect and prevent access to malicious websites	IAM-05
DS-3.0	LAN / Internal Network	Isolate the content/production network from non-production networks (e.g., office network, DMZ, the internet etc.) by means of physical or logical network segmentation.	Customers can provision separate domains or organizations with a domain for testing purposes. Google provides solution papers and reference Development and Test environments. https://cloud.google.com/solutions/devtest/ Google segregates its production environment from its corporate environment.	· 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 · Implement firewall rules to deny all outbound traffic by	IVS-08

				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 non-production networks	
DS-3.1		Restrict access to the content/productio	All access to production systems are based on least privilege, requires two-factor authentication, and is logged.	· Consider using physical Ethernet cable locks to ensure that a	IVS-11?

		n systems to authorized personnel.		network cable cannot be connected to an alternate/unauthorized device	
DS-3.2	LAN / Internal Network	Restrict remote access to the content/production network to only approved personnel who require access to perform their job responsibilities.	Google maintains an automated access revocation process that include account locking and revocation of certificates and role assignment. Google logs all changes in user permissions with the date and time of such changes.	· Prohibit remote access to the content/production network · Maintain a list of company personnel who are allowed remote access to the content/production network · Develop processes for management to review remote activity on monitor access to systems that reside on the content/production network · Configure remote access systems to use individual accounts · Limit remote access to a single method with Access Control Lists · In the event emergency remote access is required, implement the following: o Use two-factor authentication, and preferably certificate based o Block file transfer protocols including, FTP, SSH, IRC, IM o VPN configuration must not allow split tunneling o Utilize a Launchpad/bastion host model as an intermediate to connect	IAM-02

				to the production network	
DS-3.3		Use switches/layer 3 devices to manage the network traffic, and disable all unused switch ports on the content/production network to prevent packet sniffing by unauthorized devices.	cloud.google.com/docs 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 in monitored continuously. Network ACLs are documented within configuration files with comments on purpose, as appropriate. Google builds in own machines and deploys custom operating system images that only permit the necessary ports, protocols and services.	· Require that device administrators use strong authentication including: o Use of encrypted protocol o Salted hash for the password o Separate password for exec commands · Connect to the device console and update configuration files to disable unused switch ports · Enable logging on the switches/layer 3 devices	IVS-06 IVS-07
DS-3.4		Restrict the use of non-switched devices such as hubs and repeaters on the content/production network.	cloud.google.com/docs 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 in monitored continuously. Network ACLs are documented within configuration files with comments on purpose, as appropriate. Google maintains one homogeneous operating environment for Google Cloud Platform 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.	· Replace all hubs/repeats with switches or layer 3 devices	IVS-06 IVS-13?
DS-3.5	LAN / Internal Network	Prohibit dual-homed networking	cloud.google.com/docs Google maintains these diagrams for internal purposes, but due the dynamic and sensitive	· Instead use logical network bridging at the network layer (e.g.,	IVS-06 IVS-13?

		(physical networked bridging) on computer systems within the content/production network.	nature of the information, does not share it externally. The security state of network devices in monitored continuously. Network ACLs are documented within configuration files with comments on purpose, as appropriate. Google maintains one homogeneous operating environment for Google Cloud Platform 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.	routers, firewalls, switches, etc.) rather than using multiple NICs in one computer system	
DS-3.6		Implement a network-based intrusion detection /prevention system (IDS/IPS) on the content/production network.	Google does not permit wireless access in the production environment. Google has established policies and procedures to manage in corporate wireless network perimeter. Google does not permit wireless access points in its production environment. Google has established strong encryption and authentication to its corporate wireless network. Google does not permit wireless access points in its production environment and periodically scans for rogue devices. Google maintains one homogeneous operating environment for Google Cloud Platform 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.	· Configure the network-based intrusion detection/prevention system to alert on / prevent suspicious network activity · Subscribe to anti-virus/anti-malware for the IDS/IPS · Update attack signature definitions/policies and anti-virus/anti-malware on the IDS/IPS on at least a weekly basis · Log all activity and configuration changes for the IDS/IPS · Implement host-based intrusion detection system software on all workstations	IVS-12 IVS-13
DS-3.7		Disable SNMP (Simple Network	Google does not permit wireless access in the production environment. Google has	· Use an ACL that restricts access to the	IVS-12

		Management Protocol) if it is not in use or uses only SNMPv3 or higher and select SNMP community strings that are strong passwords.	established policies and procedures to manage in corporate wireless network perimeter. Google does not permit wireless access points in its production environment. Google has established strong encryption and authentication to its corporate wireless network. Google does not permit wireless access points in its production environment and periodically scans for rogue devices.	device so that only authorized management systems may be used to connect using SNMP	
DS-3.8		Harden systems prior to placing them in the LAN / Internal Network.	Google builds in own machines and deploys custom operating system images that only permit the necessary ports, protocols and services.	· Refer to DS-1.5 for suggestions	IVS-07
DS-3.9		Conduct internal network vulnerability scans and remediate any issues, at least annually.	Google performs periodic network vulnerability scans using commercial tools. Google performs periodic application-layer vulnerability scans using commercial and proprietary tools. Google performs periodic 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 monitor 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 guides. https://cloud.google.com/security/whitepaper https://cloud.google.com/terms/	· Ensure that tools used for scanning accommodate virtualization technologies, if being used · Include the following: o Production networks o Non-Production networks o Connected machines / devices o Non-connected machines / devices	TVM-02
DS-3.10	LAN / Internal Network	Secure backups of local area network SAN/NAS, devices, servers and workstations to a centrally secured server on	Customers need to manage this by leveraging the features of our storage services. Please see the product documentation for specifics: https://cloud.google.com/docs/storing-your-data Customers are primarily responsible for legal requests. Google will assist customers where necessary. Google's process for handling law enforcement requests is detailed here:	· Configure local area network devices to store backups of configuration files in a secure manner (e.g., encrypted) on the internal network	BCR-11

		the internal network.	http://www.google.com/transparencyreport/userdatarequests/legalprocess/ 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. However, 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.	· Ensure that only authorized administrators have access to the storage location and the encrypted backups	
DS-4.0	Wireless/WLAN	Prohibit wireless networking and the use of wireless devices on the content/production network.	Google does not permit wireless access in the production environment. Google has established policies and procedures to manage in corporate wireless network perimeter. Google does not permit wireless access points in its production environment. Google has established strong encryption and authentication to its corporate wireless network. Google does not permit wireless access points in its production environment and periodically scans for rogue devices. Customers can provision separate domains or organizations with a domain for testing purposes. Google provides solution papers and reference Development and Test environments. https://cloud.google.com/solutions/devtest/ Google segregates its production environment from its corporate environment.	· Restrict wireless guest networks to access only the Internet and not the content/production network · Remove or disable wireless access on workstations/laptops that process or store content in the content/production network	IVS-12 IVS-08
DS-4.1	Wireless/WLAN	Configure non-production wireless networks (e.g., administrative and guest) with the following security controls:	We encrypt data at rest in Google Cloud Platform. Network packets are encrypted when they leave Google Compute Engine Instances. Google has a service (currently in Beta) which allows customers to supply their own encryption keys via API.	· Consider security controls such as: o Use non-company specific SSID names o Enable IEEE 802.1X or IEEE 802.11i where the option is available	EKM-03 IVS-12

		· Disable WEP / WPA · Only Enable AES128 encryption (WPA2), or higher · Segregate "guest" networks from the company's other networks · Change default administrator logon credentials · Change default network name (SSID)	Google maintains internal documentation for the use of its internal proprietary key management service. Google does not permit wireless access in the production environment. Google has established policies and procedures to manage in corporate wireless network perimeter. Google does not permit wireless access points in its production environment. Google has established strong encryption and authentication to its corporate wireless network. Google does not permit wireless access points in its production environment and periodically scans for rogue devices.	o Use RADIUS for authentication where the option is available o Enable MAC address filtering o Blacklist the wireless MAC addresses of production workstations and devices · Configure the wireless access point/controller to broadcast only within the required range · Implement an 802.1X framework for wireless networking, which includes the following: o Remote Access Dial In User Service (RADIUS) for Authentication, Authorization and Accounting o Lightweight Directory Access Protocol (LDAP) server, such as Active Directory, to manage user accounts o Public Key Infrastructure to generate and manage client and server certificates · Implement the following controls if pre-shared keys must be used: o Configure WPA2 with CCMP (AES-128) encryption, or higher o Set a complex passphrase (See DS-8.1 for passphrase complexity recommendations)	

				o Change the passphrase at least every 90 days and when key company personnel terminate their employment	
DS-4.2	Wireless/WLAN	Implement a process to scan for rogue wireless access points and remediate any validated issues.	Google does not permit wireless access in the production environment. Google has established policies and procedures to manage in corporate wireless network perimeter. Google does not permit wireless access points in its production environment. Google has established strong encryption and authentication to its corporate wireless network. Google does not permit wireless access points in its production environment and periodically scans for rogue devices.	· 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	IVS-12
DS-5.0	I/O Device Security	Designate specific systems to be used for content input/output (I/O).	IO paths in all datacenters are tightly controlled and monitored	· Implement ACLs to allow traffic between the content/production network and systems used for I/O for specific source/destination IP addresses	
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.	These external IO paths are disabled in the datacenters	· Consider the following for blocking I/O devices: o Change the registry setting to restrict write access to I/O devices for MS Windows-based systems o Remove the mass storage file to control write access on production stations for Mac-based systems o Disable I/O devices using group policy for systems using Microsoft Active Directory or Apple Open Directory	

				o Use I/O port monitoring software to detect port usage if blocking output devices is not feasible	
DS-6.0	System Security	Install anti-virus and anti-malware software on all workstations, servers, and on any device that connects to SAN/NAS systems.	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 ISO27002. Google maintains an automated log collection and analysis tool to review and analyse log events. Google builds in own machines and deploys custom operating system images that only permit the necessary ports, protocols and services.	· Install an enterprise anti-virus and anti-malware solution with a centralized management console · Consider the installation of endpoint protection	IVS-01 IVS-07
DS-6.1		Update all anti-virus and anti-malware definitions daily, or more frequently.	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 27001 security objectives.	· Configure the centralized anti-virus and anti-malware management console to download and push definition updates at least once each day	
DS-6.2		Scan all content for viruses and malware prior to ingest onto the content/production network.	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 27001 security objectives.	· Perform scans on a system that is not connected to the content/production network	AIS-04?
DS-6.3	System Security	Perform scans as follows: · Enable regular full system virus and malware scanning on all workstations · Enable full system virus and	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 ISO27002.	· Configure anti-virus and anti-malware software to conduct a full system scan based upon the anti-virus and anti-malware strategy · Configure anti-virus and anti-malware software to execute during idle periods	IVS-01 IVS-07

		malware scans for servers and for systems connecting to a SAN/NAS	Google maintains an automated log collection and analysis tool to review and analyse log events. Google builds in own machines and deploys custom operating system images that only permit the necessary ports, protocols and services.		
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.	Google performs periodic network vulnerability scans using commercial tools. Google performs periodic application-layer vulnerability scans using commercial and proprietary tools. Google performs periodic 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 monitor 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 guides. https://cloud.google.com/security/whitepaper https://cloud.google.com/terms/	· Where possible, implement a centralized patch management tool (e.g., WSUS, Shavlik, Altiris) to automatically deploy patches to all systems · Seek out patches from vendors and other third parties · Test patches prior to deployment · Implement an exception process and compensating controls for cases where there is a legitimate business case for not patching systems	TVM-02
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	Google maintains an automated access revocation process that include account locking and revocation of certificates and role assignment. Google logs all changes in user permissions with the date and time of such changes.	· Ensure that the user account used to login to the workstation does not have privileges as an Administrator of the system	IAM-02

		from the software provider must explicitly state that administrative rights are required.			
DS-6.6		Use cable locks on portable computing devices that handle content (e.g., laptops, tablets, towers) when they are left unattended.	Google's defense in depth approach assumes that all devices may be compromised at any time. MFA on all systems prevents physcial loss from compromising security. Physcial security of all systems is built in to the infrastrcuture.	· Secure cable lock to a stationary object (e.g., table)	
DS-6.7	System Security	Implement additional security controls for laptops and portable computing storage devices that contain content or sensitive information relating to client projects. Encrypt all laptops. Use hardware-encrypted portable computing storage devices. Install remote-kill software on all laptops/mobile devices that handle content to allow remote wiping of hard drives and other storage devices.	Google's supports remote wipe capabilities for mobile devices with access to sensitive corporate information. We encrypt data at rest in Google Cloud Platform. Network packets are encrypted when they leave Google Compute Engine Instances. Google has a service (currently in Beta) which allows customers to supply their own encryption keys via API. Google maintains internal documentation for the use of its internal proprietary key management service.	· 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	MOS-18 EKM-03
DS-6.8		Restrict software installation privileges to IT management.	Google uses automated configuration management tools, software release tools and mobile device management software to restrict	· Prohibit the installation and usage of unapproved software including rogue	CCC-04

			and monitor the installation of unauthorized software.	software (e.g., illegal or malicious software) · Scan all systems for an inventory of installed applications at least quarterly	
DS-6.9		Implement security baselines and standards to configure systems (e.g., laptops, workstations, servers, SAN/NAS) that are set up internally.	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. 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 platform. https://cloud.google.com/compute/docs/tutorials/building-images	· Develop a secure standard build that is used to image all systems	GRM-01
DS-6.10		Unnecessary services and applications should be uninstalled from content transfer servers.	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 27001 security objectives.	· 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 non-essential applications are not running	
DS-6.11		Maintain an inventory of systems and system components.	Google maintains assets inventories and assigns ownership for managing its critical resources. Google maintains a list of Sub-Processors: https://www.google.com/intx/en/work/apps/terms/subprocessors.html	· Update the inventory on at least a monthly basis	DCS-01

DS-6.12	System Security	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. Google maintains one homogeneous operating environment for Google Cloud Platform 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.	· Include WAN, DMZ, LAN, WLAN (wireless), VLAN, firewalls, and server/network topology	BCR-04 IVS-13
DS-7.0	Account Management	Establish and implement an account management process for administrator, user, and service accounts for all information systems and applications that handle content.	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 support 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 GSuite to their existing identity management system. Customers can customize access to	· Document policies and procedures for account management which address the following: o New user requests o User access modifications o Disabling and enabling of user accounts o User termination o Account expiration o Leaves of Absence o Disallow the sharing of any user account by multiple users o Restrict the use of service accounts to only applications that require them · Enable logging on the following infrastructure systems and devices at a minimum: o Infrastructure components (e.g., firewalls, authentication servers, network operating systems, remote access	IAM-12

			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. Gsuite 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 whom 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. 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.	mechanisms including VPN) o Production operating systems o Content management components (e.g., storage devices, content servers, content storage tools, content transport tools) o Systems with Internet access o Implement a server to manage the logs in a central repository (e.g., syslog/log management server, Security Information and Event Management (SIEM) tool)	
DS-7.1	Account Management	Maintain traceable evidence of the account management activities (e.g., approval emails, change request forms).	Google maintains an automated access revocation process that include account locking and revocation of certificates and role assignment. Google logs all changes in user permissions with the date and time of such changes. Google supports integration with a customer's SSO solution:	· Retain evidence of management approvals and associated actions for all account management activities, where possible	

			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 support 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 GSuite 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. Gsuite 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 whom 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. 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-7.2		Assign unique credentials on a need-to-know basis using the principles of least privilege.	Google maintains an automated access revocation process that include account locking and revocation of certificates and role assignment. Google logs all changes in user permissions with the date and time of such changes. 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 support 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	· Assign credentials on a need-to-know basis for the following information systems, at a minimum: o Production systems o Content management tools o Content transfer tools o Network infrastructure devices o Logging and monitoring systems o Client web portal o Account management systems (e.g., Active Directory, Open Directory, LDAP) o VPN remote permissions, which should only be granted when absolutely required	IAM-02 IAM-12

			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 GSuite 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. Gsuite 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 whom 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. 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-7.3		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).		· 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	
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).	Customers can provision separate domains or organizations with a domain for testing purposes. Google provides solution papers and reference Development and Test environments. https://cloud.google.com/solutions/devtest/ Google segregates its production environment from its corporate environment.	· Leverage an independent team to grant access to information systems when possible · Implement compensating controls when segregation is unattainable, such as: o Monitor the activity of company personnel and third party workers o Retain and review audit logs o Implement physical segregation o Enforce management supervision	IVS-08
DS-7.5	Account Management	Monitor and audit administrator and service account activities.	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 ISO27002.	· 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: o User name o Time stamp	IVS-01?

			Google maintains an automated log collection and analysis tool to review and analyse log events.	o Action o Additional information (action parameters) · Monitor service accounts to ensure that they are used for intended purposes only (e.g., database queries, application-to-applicatio n communication) · Implement a monthly process to review administrator and service account activity to identify unusual or suspicious behavior and investigate possible misuse	
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.	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.	· 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 · Remove or disable accounts that have not been used in over 90 days	IAM-10
DS-7.7		Restrict user access to content on a per-project basis.	Google provides (under a specific NDA) customers with a SOC 2/3 report that includes testing of Google's access controls. Details are documented here: https://cloud.google.com/security/whitepaper	· Remove access rights to information systems from users that no longer require access due to project completion	IAM-05
DS-7.8	Account Management	Disable or remove local accounts on systems that handle content where technically feasible.	All accounts on production systems are tightly controlled. "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 27001 security objectives. "	· 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 · 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	
DS-8.0	Authentication	Enforce the use of unique usernames and passwords to access information systems.	Google's Device Policy Manager enforces password policies. User can choose their authentication setting as long as minimum requirements such as 4 point swipe pattern or PIN. Google maintains an automated access revocation process that include account locking and revocation of certificates and role assignment. Google logs all changes in user permissions with the date and time of such changes. 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 support 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	· 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	MOS-16 IAM-02 IAM-12

			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 GSuite 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. Gsuite 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 whom 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.		

			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-8.1		Enforce a strong password policy for gaining access to information systems.		· Create a password policy that consists of the following: o Minimum password length of 8 characters o Minimum of 3 of the following parameters: upper case, lower case, numeric, and special characters o Maximum password age of 90 days o Minimum password age of 1 day o Maximum invalid logon attempts of between 3 and 5 attempts o User accounts locked after invalid logon attempts must be manually unlocked, and should not automatically unlock after a certain amount of time has passed o Password history of ten previous passwords	
DS-8.2	Authentication	Implement two-factor authentication (e.g., username/password and hard token) for remote access (e.g., VPN) to the networks.	Google maintains an automated access revocation process that include account locking and revocation of certificates and role assignment. Google logs all changes in user permissions with the date and time of such changes.	· Require individuals to provide two of the following for remote access: o Information that the individual knows (e.g., username, password) o A unique physical item that the individual has (e.g., token,	IAM-02

				keycard, smartphone, certificate) o 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) at 128 bits or higher to carryout remote administration functions	
DS-8.3		Implement password-protected screensavers or screen-lock software for servers and workstations.	Google's Device Policy Manager requires personnel to set an automatic lockout screen.	· 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	MOS-14
DS-8.4		Consider implementing additional authentication mechanisms to provide a layered authentication strategy for WAN and LAN / Internal Network access.	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 support 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	· Consider adding one or more of the following: o Multi-factor authentication o Identity and access management system o Single sign on system o Identity federation standards	IAM-12

			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 GSuite 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. Gsuite 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 whom 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. 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-9.0	Logging and Monitoring	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)	Google machine configuration changes are continuously monitored when online. Google Cloud platform provides the ability to log and monitor the health of virtual instances using variety of tools : https://console.developers.google.com https://cloud.google.com/docs/	· Enable logging on the following infrastructure systems and devices at a minimum: o Infrastructure components (e.g., firewalls, authentication servers, network operating systems, remote access mechanisms (e.g., VPN systems) o Production operating systems o Content management components (e.g., storage devices, content servers, content storage tools, content transport tools) o Systems with Internet access o Applications	IVS-02
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).	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 27001 security objectives.		
DS-9.2		Configure logging systems to send automatic notifications when security events are detected in order to facilitate active response to incidents.	Google maintains one homogeneous operating environment for Google Cloud Platform 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	· Define events that require investigation and enable automated notification mechanisms to appropriate personnel; consider the following: o Successful and unsuccessful attempts to connect to the content/production network	IVS-13 SEF-02 SEF-05

			3. Employing technologies that automatically remedy certain dangerous situations. Google maintains incident response procedures to help ensure prompt notification and investigation of incidents. Google has a 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. 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. 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. https://cloud.google.com/terms/ 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.	o Unusual file size and/or time of day transport of content o Repeated attempts for unauthorized file access o 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)	

			Should the amount of data increase, Google will consider sharing this statistical information.		
DS-9.3		Investigate any unusual activity reported by the logging and reporting systems.	Google maintains incident response procedures to help ensure prompt notification and investigation of incidents. Google has a 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. 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. 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. https://cloud.google.com/terms/ Google performs annual testing of its emergency response processes.	· Incorporate incident response procedures for handling detected security events	SEF-02
DS-9.4	Logging and Monitoring	Implement logging mechanisms on all systems used for the following:	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.	· Ensure that all generated keys and added certificates are traceable to a unique user	EKM-02

		· Key generation · Key management · Vendor certificate management	Google has a service (currently in Beta) which allows customers to supply their own encryption keys via API. Google maintains documentation on its key management process. Google maintains documentation on its key management process and provides controls to manage encryption keys through their lifecycle and protect against unauthorized use. Google uses a combination of open source and proprietary code to develop its encryption solutions		
DS-9.4		Review all logs weekly, and review all critical and high daily.	Google maintains incident response procedures to help ensure prompt notification and investigation of incidents. Google has a 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. 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. Due to the fact that the incident response system is standardized, customization of the	· 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	SEF-02

			notification process is not supported for each tenant. The terms of service cover roles and responsibilities. https://cloud.google.com/terms/ Google performs annual testing of its emergency response processes.		
3		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)	Google maintains incident response procedures to help ensure prompt notification and investigation of incidents. Google has a 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. 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. 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. https://cloud.google.com/terms/ Google performs annual testing of its emergency response processes.		SEF-02

DS-9.6	Logging and Monitoring	Retain logs for at least one year.	Google maintains incident response procedures to help ensure prompt notification and investigation of incidents. Google has a 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. 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. 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. https://cloud.google.com/terms/ Google performs annual testing of its emergency response processes.	· 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	SEF-02
DS-9.7		Restrict log access to appropriate personnel.	Google maintains an automated access revocation process that include account locking and revocation of certificates and role assignment. Google logs all changes in user permissions with the date and time of such changes.	· Maintain Access Control Lists to ensure that only personnel responsible for log monitoring and review have permission to view logs	IAM-02

				· 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	
DS-10.0	Mobile Security	Develop a BYOD (Bring Your Own Device) policy for mobile devices accessing or storing content.	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.	· Consider implementing mobile device anti-virus/anti-malware protection including: o Update definitions including o Perform scans daily	MOS-08
DS-10.1		Develop a list of approved applications, application stores, and application plugins/extensions for mobile devices accessing or storing content.	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.	· 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	MOS-04
DS-10.2		Maintain an inventory of all mobile devices that access or store content.	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.	· Include operating system, patch levels, applications installed	MOS-09 MOS-10
DS-10.3		Require encryption either for the entire device or for areas of the device where content will be handled or stored.	Mobile devices with access to corporate resources other than Apps services require encryption.	· Consider a mobile device management system	MOS-11

DS-10.4		Prevent the circumvention of security controls.	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 the the required security specifications. The Device Policy Manager is required in order to access corporate sources using mobile applications.	· Prevent the use of jailbreaking, rooting etc.	MOS-12
DS-10.5	Mobile Security	Implement a system to perform a remote wipe of a mobile device, should it be lost / stolen / compromised or otherwise necessary.	Google's supports remote wipe capabilities for mobile devices with access to sensitive corporate information.	· Remind employees that non-company data may be lost in the event a remote wipe of a device is performed	MOS-18
DS-10.6		Implement automatic locking of the device after 10 minutes of non-use.	Google's Device Policy Manager requires personnel to set an automatic lockout screen.		MOS-14
DS-10.7		Manage all mobile device operating system patches and application updates.	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.	· Apply the latest available security-related patches/updates upon general release by the device manufacturer, carrier or developer	MOS-19
DS-10.8		Enforce password policies.	Google's Device Policy Manager enforces password policies. User can choose their authentication setting as long as minimum requirements such as 4 point swipe pattern or PIN.	· Refer to DS-8.1	MOS-16
DS-10.9		Implement a system to perform backup and restoration of mobile devices.	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 but requires a device configuration and uses reduces the risk of malware from being installed on the device.	· Encrypt backups and store them in a secure location	MOS-17
DS-11.0	Security Techniques	Ensure that security techniques (e.g.,	Google defines a data security architecture conducive to its operational needs and has demonstrated that this architecture satisfies		

		spoiling, invisible/visible watermarking) are available for use and are applied when instructed.	industry standards such as FedRamp, NIST 800-53, SOC 2/3 and ISO 27001 security objectives.		
DS-11.1		Encrypt content on hard drives or encrypt entire hard drives using a minimum of AES 128-bit, or higher, encryption by either: · File-based encryption: (i.e., encrypting the content itself) · Drive-based encryption: (i.e., encrypting the hard drive)	We encrypt data at rest in Google Cloud Platform. Network packets are encrypted when they leave Google Compute Engine Instances. Google has a service (currently in Beta) which allows customers to supply their own encryption keys via API. Google maintains internal documentation for the use of its internal proprietary key management service.	· For external hard drives, consider purchasing pre-encrypted drives (e.g., Rocstor Rocsafe, LaCie Rugged Safe) · Encrypt all content on hard drives including: o SAN / NAS o Servers o Workstations o Desktops o Laptops o Mobile devices o External storage drives · Implement one or more of the following: o File-based encryption such as encrypted DMGs or encrypted ZIP files o Drive-based encryption using software	EKM-03
DS-11.2		Send decryption keys or passwords using an out-of-band communication protocol (i.e., not on the same storage media as the content itself).	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.	· 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	EKM-04
DS-11.3	Security Techniques	Implement and document key management policies and procedures:	Google maintains documentation on its key management process and provides controls to manage encryption keys through their lifecycle and protect against unauthorized use.	· Consider the creation of unique encryption keys per client and for critical assets	EKM-01

		· 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		· Prevent unauthorized substitution of cryptographic keys · Require cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities	
DS-11.4		Encrypt content at rest and in motion, including across virtual server instances, using a minimum of AES 128-bit, or higher, encryption.	We encrypt data at rest in Google Cloud Platform. Network packets are encrypted when they leave Google Compute Engine Instances. Google has a service (currently in Beta) which allows customers to supply their own encryption keys via API.	· http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf	EKM-03

			Google maintains internal documentation for the use of its internal proprietary key management service.		
DS-11.5	Security Techniques	Store secret and private keys (not public keys) used to encrypt data/content in one or more of the following forms at all times: · Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key · Within a secure cryptographic device (e.g., Host Security Module (HSM) or a Pin Transaction Security (PTS) point-of-interaction device) o 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.		EKM-04
DS-11.6		Confirm that devices on the Trusted Devices List (TDL) are appropriate based on rights owners' approval.	Google maintains a mobile device policy that details our requirements for mobile device use at Google. Customer data is not permitted on mobile devices.	· 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	HRS-05

DS-11.7		Confirm the validity of content keys and ensure that expiration dates conform to client instructions.	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 27001 security objectives.	· 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	
DS-12.0	Content Tracking	Implement a digital content management system to provide detailed tracking of digital content.	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 27001 security objectives.	· 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	
DS-12.1	Content Tracking	Retain digital content movement transaction logs for one year.	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 27001 security objectives.	· Include the following: o Time and date of check-in/check-out o Name and unique id of the individual who checked out an asset o Reason for check-out o Location of content	
DS-12.2		Review logs from digital content management system periodically and investigate anomalies.	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 27001 security objectives.		
DS-12.3		Use client AKAs (“aliases”) when applicable in digital asset tracking systems.	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 27001 security objectives.	· Restrict knowledge of client AKAs to personnel involved in processing client assets	
DS-13.0	Transfer Systems	Use only client-approved transfer systems that utilize access	Google defines a data security architecture conducive to its operational needs and has demonstrated that this architecture satisfies industry standards such as FedRamp, NIST	· Allow only authorized users to have access to the content transfer system	

		controls, a minimum of AES 128-bit, or higher, encryption for content at rest and for content in motion and use strong authentication for content transfer sessions.	800-53, SOC 2/3 and ISO 27001 security objectives.	· Consider restricting access also on a project basis · Verify with the client that the content transfer systems are approved, prior to use	
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.	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 27001 security objectives.	· 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	
DS-14.0	Transfer Device Methodology	Implement and use dedicated systems for content transfers.	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 27001 security objectives.	· 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	
DS-14.1		Separate content transfer systems from administrative and production networks.	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 27001 security objectives.	· Separate networks either physically or logically	
DS-14.2	Transfer Device Methodology	Place content transfer systems in a Demilitarized	Google defines a data security architecture conducive to its operational needs and has demonstrated that this architecture satisfies	· Harden content transfer systems prior to placing them in the	

		Zone (DMZ) and not in the content/production network.	industry standards such as FedRamp, NIST 800-53, SOC 2/3 and ISO 27001 security objectives.	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 · 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	
DS-14.3		Remove content from content transfer devices/systems immediately after successful transmission/receipt.	This falls under the shared security model and falls on the client systems.	· 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	
DS-14.4		Send automatic notifications to the production coordinator(s) upon outbound		· Configure the content transfer system to send an automatic notification (e.g., an email) to the production	

		content transmission.		coordinator(s) each time a user sends content out of the network	
DS-15.0	Client Portal	Restrict access to web portals which are used for transferring content, streaming content and key distribution to authorized users.		· Implement access control measure around web portals that transfer content, stream content and distribute keys by implementing one or more of the following: o Require user credentials o Integrate machine and/or user keys for authentication and authorization o 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) o Limit portal access to specific networks, VLANs, subnets, and/or IP address ranges o Restrict the ability to upload/download as applicable from the client portal	
DS-15.1	Client Portal	Assign unique credentials (e.g., username and password) to portal users and distribute credentials to clients securely.		· Do not embed user names and passwords in content links · Consider distributing the user credentials and content links in separate emails · Consider distributing user credentials via phone or SMS	

				· Consider distributing encryption keys via out of band transfer · Create a password policy that consists of the following: o Minimum password length of 8 characters o Minimum of 3 of the following parameters: upper case, lower case, numeric, and special characters o Maximum password age of 90 days o Minimum password age of 1 day o Maximum invalid logon attempts of between 3 and 5 attempts o User accounts locked for invalid logon attempts should be manually unlocked, and should not automatically unlock after a certain amount of time has passed o Password history of ten previous passwords	
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).		· Implement a process to review file/directory permissions at least quarterly · Ensure that access is restricted to only those that require it	
DS-15.3		Place the web portal on a dedicated server in the DMZ and limit access to/from specific IPs and protocols.		· 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)	
DS-15.4	Client Portal	Prohibit the use of third-party production software/systems/ services that are hosted on an internet web server unless approved by client in advance.		· Consider adding one or more of the following: o Multi-factor authentication o Identity and access management system o Single sign on system o Identity federation standards o Use a VPN connection with advanced encryption standard (AES) at 128 bits or higher	
DS-15.5		Use HTTPS and enforce use of a strong cipher suite (e.g., TLS v1) for the internal/external web portal.	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 27001 security objectives.		
DS-15.6		Do not use persistent cookies or cookies that store credentials in plaintext.	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 27001 security objectives.	· 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: o Reconfigure the application o Update the application	

				o 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.			
DS-15.8		Test for web application vulnerabilities quarterly and remediate any validated issues.		· 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 Appendix G for further information	
DS-15.9	Client Portal	Perform annual penetration testing of web applications and remediate any validated issues.		· 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 Appendix G for further information	
DS-15.10		Allow only authorized personnel to request the establishment of a connection with the telecom service provider.			
DS-15.11		Prohibit transmission of content using email (including webmail).		· 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)	
DS-15.12		Review access to the client web portal at least quarterly.		· 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	