FISC Security Guidelines 11th Edition (revised May 2023)

Handbook for Google Cloud and Google Workspace

This document provides an overview of the security management measures implemented by Google Cloud and Google Workspace as a part of the information disclosure requirement under “FISC Security Guideline 11th Edition (revised May 2023)” required by FISC.
Google's controls described in this document are certified by the third-party audit compliance programs ISO / IEC 27001, ISO / IEC 27017, and ISO / IEC 27018.
This handbook explains how customers confirm Google Cloud services and related compliance programs ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 so that they can meet the requirements.

Control number is compliant with the FISC guidelines. Items to be implemented within the scope of customer's responsibility are described as "-".

Control no.	Google Response	Google Cloud Financial Services Contract reference
C1	-	-
C2	-	-
C3	-	-
C4	-	-
C5	-	-
C6	-	-
C7	-	-
C8	-	-
C9	-	-
C10	-	-
C11	-	-
C12	-	-
C13	-	-
C14	-	-
C15	-	-
C16	-	-
C17	-	-
C18	-	-
C19	-	-
C20	It is the customer's responsibility to conduct an appropriate evaluation when selecting a cloud provider. Google provides resources to help customers evaluate the suitability of Google Cloud and Google Workspace as external providers. ◯ Compliance Google Cloud Compliance https://cloud.google.com/security/compliance Latest Compliance Offerings https://cloud.google.com/security/compliance/offerings ◯ Google Cloud Terms of Service Overview of Google Cloud Platform Services https://cloud.google.com/terms/services Google Cloud Platform Service Level Agreements https://cloud.google.com/terms/sla/ Overview of Google Workspace https://workspace.google.co.jp/intl/ja/terms/user_features.html Google Workspace Service Level Agreements https://workspace.google.com/terms/sla.html	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
C20 (cont.)	Google Cloud Service-Specific Terms https://cloud.google.com/terms/service-terms Google Workspace Service-Specific Terms https://workspace.google.co.jp/intl/ja/terms/service-terms/index.html Data Processing and Security Terms https://cloud.google.com/terms/data-processing-terms#top_of_page Data Processing and Security Terms (Data Transfers) https://cloud.google.com/terms/data-processing-addendum#10.-data-transfers Google Cloud Subprocessors https://cloud.google.com/terms/subprocessors Google Workspace and Cloud Identity Subprocessors https://workspace.google.com/terms/subprocessors.html Technical Support Services Guidelines https://cloud.google.com/terms/tssg/ ◯Google Cloud Security Google Security Whitepaper https://cloud.google.com/security/overview/whitepaper Cloud-Native Security Whitepaper https://cloud.google.com/security/beyondprod Google Workspace Security Whitepaper https://static.googleusercontent.com/media/workspace.google.com/en//intl/ja/files/google-apps-security-and-compliance-whitepaper.pdf Infrastructure Security https://cloud.google.com/security/infrastructure/ Infrastructure Security Design Overview https://cloud.google.com/security/infrastructure/design/ Security Resources https://cloud.google.com/security Cloud Security Products https://cloud.google.com/products/security-and-identity Security Best Practices https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#networking-and-security Security Use Cases https://cloud.google.com/security/showcase/	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
C20 (cont.)	◯ Google Cloud Locations Google Cloud Locations https://cloud.google.com/about/locations/ Google Cloud Whitepaper on Data Residency, Operational Transparency, and Customer Privacy https://services.google.com/fh/files/misc/googlecloud_european_commitments_whitepaper.pdf ◯ Google Cloud Disaster Recovery and Incident Management Disaster Recovery Building Blocks https://cloud.google.com/architecture/dr-scenarios-building-blocks Disaster Recovery Planning Guide https://cloud.google.com/architecture/dr-scenarios-planning-guide Disaster Recovery Scenarios for Data https://cloud.google.com/architecture/dr-scenarios-for-data Incidents and the Google Cloud Status Dashboard https://cloud.google.com/support/docs/dashboard Data Incident Response Whitepaper https://services.google.com/fh/files/misc/data_incident_response_2018.pdf Google Cloud Status Dashboard https://status.cloud.google.com/ ◯ Data Deletion Data Deletion on the Google Cloud Platform Whitepaper https://cloud.google.com/security/deletion ◯ Support Google Cloud Support https://cloud.google.com/support-hub Language Support https://cloud.google.com/support/docs/language-working-hours ◯ Corporate Information Alphabet Investor Relations https://abc.xyz/investor/ Subprocessors https://workspace.google.com/intl/en/terms/subprocessors.html	-
C21	Google concludes the Google Cloud Financial Services Contract with regulated entities.	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
1.	The Google Cloud Financial Services Contract addresses each of the items in the framework. To assist you, we've provided information for each of the areas you need to consider in the rows that follow. Changes to contract For more information on changes to the contract refer to 1.(1), 6). For more information on changes to the service refer to 1.(1), 7).	-
1. (1)	-	-
1.(1),1)	The roles and responsibilities of the parties, definition of terms, and governing law are set out in the Google Cloud Financial Services Contract. Damages are also addressed in the Google Cloud Financial Services Contract. In particular, if Google's performance of the Services does not meet the Google Cloud Service Level Agreements regulated entities may claim service credits. Google Cloud Service Level Agreements https://cloud.google.com/terms/sla/ The governing law can be set as Japanese law, and the court of jurisdiction can be set as the Tokyo District Court.	Definitions; Liability; Governing Law Services
1.(1), 2)	-	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
1.(1), 3)	Quality You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. Verification Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: ISO/IEC 27001 https://cloud.google.com/security/compliance/iso-27001/ ISO/IEC 27017 https://cloud.google.com/security/compliance/iso-27017/ ISO/IEC 27018 https://cloud.google.com/security/compliance/iso-27018/ PCI DSS https://cloud.google.com/security/compliance/pci-dss SOC 1 https://cloud.google.com/security/compliance/soc-1 SOC 2 https://cloud.google.com/security/compliance/soc-2 SOC 3 https://cloud.google.com/security/compliance/soc-3 You can review Google's current certifications and audit reports at any time. https://cloud.google.com/security/compliance/offerings/#/	Ongoing Performance Monitoring Certifications and Audit Reports

Control no.	Google Response	Google Cloud Financial Services Contract reference
1.(1), 4)	Working hours The SLAs contain Google's commitments regarding availability of the Services. They are available on the Google Cloud Service Level Agreements page. Accessible locations To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities. Information about the location of Google's facilities and where individual Google Cloud services can be deployed is available on our Global Locations page. Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors page. Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular: The same robust security measures apply to all Google facilities, regardless of country / region. Google makes the same commitments about all its subprocessors, regardless of country / region. Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s). You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper. Google Cloud Service Level Agreements https://cloud.google.com/terms/sla/ Google Workspace Service Level Agreements https://workspace.google.com/terms/sla.html Global Locations https://cloud.google.com/about/locations/ Google Cloud subprocessors https://cloud.google.com/terms/subprocessors Google Workspace and Cloud Identity Subprocessors https://workspace.google.com/intl/en/terms/subprocessors.html Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper. https://services.google.com/fh/files/misc/googlecloud_european_commitments_whitepaper.pdf	Services Data Location (Service Specific Terms) https://cloud.google.com/terms/service-terms Data Security; Subprocessors (Data Processing and Security Terms) https://cloud.google.com/terms/data-processing-addendum#appendix-2-security-measures Data Transfers (Data Processing and Security Terms) https://cloud.google.com/terms/data-processing-addendum#appendix-2-security-measures
1.(1), 5)	Refer to your Google Cloud Financial Services Contract.	Use Restrictions
1.(1), 6)	As services and technology change, Google may update certain terms at URLs that apply to all our customers. Any updates must meet strict criteria. For example, they must not result in a material degradation of the overall security of the services or have a material adverse impact on your existing rights. Beyond these limited updates, any contract changes must be made in writing and signed by both parties.	Changes to Terms; Amendments

Control no.	Google Response	Google Cloud Financial Services Contract reference
1.(1), 7)	Google continuously updates the services to enable our customers to take advantage of the most up-to-date technology. Given the one-to-many nature of our service, updates apply to all customers at the same time. Google will not make updates that materially reduce the functionality, performance, availability or security of the Services. If Google needs to discontinue a service without replacing it, you will receive at least 12 months' advance notice. Google will continue to provide support and product and security updates during this period.	Changes to Services
1. (2)	Service specifications The Google Cloud services are described on our services summary page. The Google Workspace services are described on our services summary page. Data protection This is addressed in the Data Processing and Security Terms where Google makes commitments to protect your data, including regarding security, use, incidents, access and retention. Google Cloud Platform Services Summary https://cloud.google.com/terms/services Google Workspace Services Summary https://workspace.google.com/terms/user_features.html Cloud Data Processing Addendum (Customers) https://cloud.google.com/terms/data-processing-terms#top_of_page	Definitions Data Security; Security Measures (Data Processing and Security Terms) https://cloud.google.com/terms/data-processing-addendum#appendix-2-security-measures
1.(2), 1)	Fees Refer to your Google Cloud Financial Services Contract. Expiry Refer to your Google Cloud Financial Services Contract.	Payment Terms Term and Termination
1.(2), 2)	Refer to 1. (2) for a description of the Google Cloud services. The customer decides which services to use, how to use them and for what purpose. Therefore the customer stays in control of the relevant activities.	-
1.(2), 3)	Refer to 1. (2) for a description of the Google Cloud services and 1.(1), 7) on service modifications.	-
1.(2), 4)	Refer to your Google Cloud Financial Services Contract.	Confidentiality
1.(2), 5)	Google will ensure its employees comply with Google's security measures and that all personnel authorized to process customer data are under an obligation of confidentiality. Trusted infrastructure https://cloud.google.com/security/infrastructure	Data Security; Security Compliance by Google Staff (Data Processing and Security Terms) https://cloud.google.com/terms/data-processing-addendum#appendix-2-security-measures

Control no.	Google Response	Google Cloud Financial Services Contract reference
1.(2), 6)	The security of a cloud service consists of two key elements: (1) Security of Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers. Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis. More information is available at: Our infrastructure security page Our security whitepaper Our cloud-native security whitepaper Our infrastructure security design overview page Our security resources page Infrastructure security https://cloud.google.com/security/infrastructure/ Security whitepaper https://cloud.google.com/docs/security/overview/whitepaper Cloud-native security whitepaper https://cloud.google.com/security/beyondprod Infrastructure security design overview page https://cloud.google.com/security/infrastructure/design/ Security resources https://cloud.google.com/security/ Security and identity https://cloud.google.com/products/security-and-identity In addition, you can review Google's SOC 2 report.	Data Security; Security Measures (Data Processing and Security Terms) https://cloud.google.com/terms/data-processing-addendum#appendix-2-security-measures

Control no.	Google Response	Google Cloud Financial Services Contract reference
1.(2), 6) (cont.)	(2) Security of your data and applications in the cloud You define the security of your data and applications in the cloud. This refers to the security measures that you choose to implement and operate when you use the Services. (a) Security by default Although we want to offer you as much choice as possible when it comes to your data, the security of your data is of paramount importance to Google and we take the following proactive steps to assist you: Encryption at rest. Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available at: https://cloud.google.com/security/encryption-at-rest/default-encryption Encryption in transit. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available at https://cloud.google.com/security/encryption-in-transit (b) Security products In addition to the other tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available on our Cloud Security Products page. (c) Security resources Google also publishes guidance on: Security best practices Security use cases Security best practices,security use cases https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#networking-and-security	Data Security; Security Measures (Data Processing and Security Terms) https://cloud.google.com/terms/data-processing-addendum#appendix-2-security-measures
1.(2), 7)	Regulated entities can use Cloud Storage as part of their backup routine. Refer to our Disaster Recovery Building Blocks and Disaster Recovery Scenarios for Data articles for more information about how you can use the services for data backup. Cloud Storage https://cloud.google.com/storage Disaster Recovery Building Blocks https://cloud.google.com/solutions/dr-scenarios-building-blocks Disaster Recovery Scenarios https://cloud.google.com/solutions/dr-scenarios-for-data	Customer's Security Responsibilities

Control no.	Google Response	Google Cloud Financial Services Contract reference
1. (3)	You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. If Google's performance of the Services does not meet the Google Cloud Service Level Agreements regulated entities may claim service credits. Google Cloud Platform Service Level Agreements https://cloud.google.com/terms/sla/ Google Workspace Service Level Agreement https://workspace.google.com/terms/sla.html	Ongoing Performance Monitoring Services
1. (4)	Information Google commits to only access or use your data to provide the Services ordered by you and will not use it for any other Google products, services, or advertising. Cooperation with supervisory authorities Google grants audit, access and information rights to supervisory authorities and their appointees. This includes access to both documentation and information and the right to conduct onsite visits. Google will fully cooperate with supervisory authorities exercising their audit, information and access rights. Reporting, communication and Incident Response Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available on our Incidents & the Google Cloud dashboard page In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper. Incidents & the Google Cloud dashboard https://cloud.google.com/support/docs/dashboard Google Workspace Status Dashboard https://www.google.com/appsstatus/dashboard/ Data incident response https://cloud.google.com/docs/security/incident-response	Protection of Customer Data Regulator Information, Audit and Access Enabling Customer Compliance Significant Developments Data Incidents (Data Processing and Security Terms) https://cloud.google.com/terms/data-processing-addendum#appendix-2-security-measures

Control no.	Google Response	Google Cloud Financial Services Contract reference
1.(4), 1)	You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: Service Health provides status information on the Services. Cloud Monitoring is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud. Google Workspace Status Dashboard provides the current and past status of core Google Workspace services, such as Gmail, Google Calendar, and Google Meet. Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). Google Cloud Service Health https://status.cloud.google.com/ Cloud Monitoring https://cloud.google.com/monitoring Google Workspace Status Dashboard https://www.google.co.jp/appsstatus/dashboard/ Access Transparency https://cloud.google.com/assured-workloads/access-transparency/docs/overview	Ongoing Performance Monitoring
1.(4),2)	You can provide Google instructions about your data and Google will comply with those instructions. Regulated entities can use the following functionality to provide instructions to Google about the Services: Cloud Console: A web-based graphical user interface that customers can use to manage their Google Cloud resources. gcloud Command Tool: A tool that provides the primary command-line interface to Google Cloud. A command-line interface is a user interface to a computer's operating system. Google APIs: Application programming interfaces which provide access to Google Cloud. Cloud Console https://cloud.google.com/cloud-console gcloud Command Tool https://cloud.google.com/sdk/gcloud Google Cloud APIs https://cloud.google.com/apis/docs/overview	Google's Compliance with Instructions (Data Processing and Security Terms) https://cloud.google.com/terms/data-processing-addendum#appendix-2-security-measures
1.(4),3)	Refer to your Google Cloud Financial Services Contract.	Governing Law

Control no.	Google Response	Google Cloud Financial Services Contract reference
1.(4),4)	In addition to the support services described on our technical support services guidelines page, Google provides documentation to explain how regulated entities and their employees can use our services. In particular, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide. If a regulated entity would like more guided training, Google also provides a variety of courses and certifications. Technical support services guidelines https://cloud.google.com/terms/tssg/ Google Cloud documents https://cloud.google.com/docs Disaster Recovery Planning Guide https://cloud.google.com/architecture/dr-scenarios-planning-guide Google Cloud trainigs and certifications https://cloud.google.com/training#overview	Technical Support
1.(4),5)	Information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide. In particular, refer to the Architecting disaster recovery for cloud infrastructure outages article for information about how you can achieve your desired RTO and RPO for your applications. Disaster Recovery Planning Guide https://cloud.google.com/architecture/dr-scenarios-planning-guide Architecting disaster recovery for cloud infrastructure outages https://cloud.google.com/architecture/disaster-recovery Google Workspace security whitepaper https://workspace.google.com/learn-more/security/security-whitepaper/page-4.html	Business Continuity and Disaster Recovery
1.(4),6)	For more information on Google's process for reporting incidents refer to 1. (4).	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
1.(4),7)	For more information on Google's process for reporting incidents refer to 1. (4). In addition, Google recognizes that you need visibility into who did what, when, and where for all user activity on our service. Cloud Audit Logs help your security teams maintain audit trails in Google Cloud and view detailed information about Admin activity, data access, and system events. In addition, you can also monitor and control the limited actions performed by Google personnel on your data using these tools: Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). Access Approval is a feature that enables you to require your explicit approval before Google support and engineering teams are permitted access to your customer content. Access Approval provides an additional layer of control on top of the transparency provided by Access Transparency. Cloud Audit Logs https://cloud.google.com/audit-logs/ Access Transparency https://cloud.google.com/logging/docs/audit/access-transparency-overview Access transparency: See logs of how Google accesses your content https://support.google.com/a/answer/9230474 Access Approval overview https://cloud.google.com/access-approval/docs/overview	-
1.(4),8)	Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide. Disaster Recovery Planning Guide https://cloud.google.com/solutions/dr-scenarios-planning-guide	Business Continuity and Disaster Recovery
1. (5)	Google will comply with all laws and regulations applicable to it in the provision of the Services. You can review information about our mission, philosophies and culture on Alphabet's Investor Relations page. It also provides information about our organisational policies e.g. our Code of Conduct. Investor Updates - Alphabet Investor Relations https://abc.xyz/investor/	Representations and Warranties

Control no.	Google Response	Google Cloud Financial Services Contract reference
1. (6)	Termination Regulated entities can elect to terminate our contract for convenience with advance notice, including if necessary to comply with law. In addition, regulated entities may terminate our contract with advance notice for Google's material breach after a cure period, for change in control or for Google's insolvency. Deletion On termination of the contractual relationship, Google will comply with your instruction to delete Customer Data from Google systems. For more information about deletion refer to our Deletion on Google Cloud whitepaper. Data deletion on Google Cloud https://cloud.google.com/docs/security/deletion Transition assistance For more information on how Google can assist on transition of the service to another service provider or back to the regulated entity refer to 1.(6), 3). Advance notice due to termination of service deprecation Regulated corporations can decide on the advance notice period associated with the termination of service deprecation by entering into a direct contract with Google.	Term and Termination Deletion on Termination (Data Processing and Security Terms) https://cloud.google.com/terms/data-processing-addendum#appendix-2-security-measures
1.(6), 1)	For more information on the regulated entity's ability to terminate the contract refer to 1.(6)	-
1.(6), 2)	On termination of the contractual relationship, Google will comply with the regulated entity's instruction to delete Customer Data from Google's systems. For more information about deletion refer to our Deletion on Google Cloud and Google Workspace whitepaper. Data deletion on Google Cloud https://cloud.google.com/security/deletion Google Workspace Security Whitepaper https://workspace.google.com/intl/ja/files/google-apps-security-and-compliance-whitepaper.pdf	Deletion on Termination (Data Processing and Security Terms) https://cloud.google.com/terms/data-processing-addendum#appendix-2-security-measures

Control no.	Google Response	Google Cloud Financial Services Contract reference
1.(6), 3)	Google recognises that regulated entities need sufficient time to exit our services (including to transfer services to another service provider). To help regulated entities achieve this, upon request, Google will continue to provide the services for 12 months beyond the expiry or termination of the contract. Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example: Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. Migrate for Anthos allows you to move and convert workloads directly into containers in Google Kubernetes Engine. You can export/import an entire VM image in the form of a .tar archive. Find more information on images and storage options on our Compute Engine Documentation page. The Data Export tool exports all supported data for all users. You can then selectively download exported data by user and service. Our Services enable you to transfer your data independently. You do not need Google's permission to do this. However, if a regulated entity would like support, upon request, Google will provide advisory and implementation services to assist in migrating workloads or otherwise transitioning use of the Services. The most scalable and fully automated Kubernetes service https://cloud.google.com/kubernetes-engine Migrate to Container https://cloud.google.com/migrate/containers OS Images https://cloud.google.com/compute/docs/images Google Workspace : Export all your organization's data https://support.google.com/a/answer/100458	Transition Term Data Export (Data Processing and Security Terms) https://cloud.google.com/terms/data-processing-addendum#appendix-2-security-measures Transition Assistance
1. (7)	Refer to your Google Cloud Financial Services Contract.	Liability
1. (8)	You retain all intellectual property rights in your data, the data you derive from your data using our services and your applications. Google commits to only access or use your data to provide the Services ordered by you and will not use it for any other Google products, services, or advertising.	Intellectual Property Protection of Customer Data
1. (9)	-	-
1. (9), 1)	Google commits to only access or use your data to provide the Services ordered by you and will not use it for any other Google products, services, or advertising.	Protection of Customer Data; Confidentiality
1. (9), 2)	For more information on Google's reporting, communication and incident response refer to 1. (4).	-
1. (10)	-	-
1. (10)	-	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
1. (11)	-	-
1. (11), 1)	Google recognizes that regulated entities need to consider the risks associated with subcontracting. We also want to provide you and all our customers with the most reliable, robust and resilient service that we can. In some cases there may be clear benefits to working with other trusted organizations e.g. to provide 24/7 support. To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will: provide information about our subcontractors; provide advance notice of changes to our subcontractors; and give regulated entities the ability to terminate if they have concerns about a new subcontractor. Google requires our subcontractors to meet the same high standards that we do. In particular, Google requires our subcontractors to comply with our contract with you. Before engaging a subcontractor, Google will conduct an assessment considering the risks related to subcontractor and the function to be subcontracted to confirm that the subcontractor is suitable.	Google Subcontractors
1. (11), 2)	Google will remain accountable to you for the performance of all subcontracted obligations.	Google Subcontractors
1. (11), 3)	Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you (including the audit and access rights, and security requirements).	Google Subcontractors
1. (11), 4)	Regulated entities should have a choice about the parties who provide services to them. To ensure this, regulated entities have the choice to terminate our contract if they think that a subcontractor change materially increases their risk or if they do not receive the agreed notice.	Google Subcontractors
1. (12)	-	-
1. (12), 1)	Google grants audit, access and information rights to regulated entities, supervisory authorities and both their appointees.	Regulator Information, Audit and Access; Customer Information, Audit and Access
1. (12), 2)	Google is committed to supporting regulated entities with audits or examinations of our services. As this support is not included in our usual publicly listed service fees, Google may charge an additional fee in connection with an audit or examination. Google will provide further details of any fee in advance of the activity when the scope of the activity is known.	Enabling Customer Compliance; Fees
1. (12), 3)	Google is committed to supporting regulated entities with audits or examinations of our services and will fully cooperate with regulated entities exercising their audit, information and access rights.	Enabling Customer Compliance
1. (13)	-	-
1. (13), 1)	Google grants audit, access and information rights to regulated entities and their appointees. This includes access to both documentation and information and the right to conduct onsite visits.	Customer Information, Audit and Access
1. (13), 2)	Prior discussions about scope will enable Google to deliver an effective audit. For example, we can ensure the relevant Google experts are available and prepared to make the most of your time. Notice also enables Google to plan the audit so that it does not create undue risk to your environment or that of any other Google customer.	Arrangements
1. (13), 3)	Regulated entities may access their data on the services at any time and may provide their supervisory authority with access. For more information on site visits and prior discussion refer to 1. (13), 2).	-
1. (14)	-	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
1. (14)	For more information about deletion, including secure decommissioning when physical storage media reaches the end of its life-cycle refer to our Deletion on Google Cloud whitepaper. Deletion on Google Cloud https://cloud.google.com/docs/security/deletion	Data Deletion (Data Processing and Security Terms)
1. (15)		Technical Support
1. (15)	Our support services are available in Japanese language. For more information about our language support refer to our Language Support page. Language support and working hours https://cloud.google.com/support/docs/language-working-hours	-
1. (16)	-	-
1. (16)	For more information on Google's reporting, communication and data incident response refer to 1.(6), 3). For more information about traceability refer to 1.(4),7).	-
1. (17)	To protect customer data, Google Cloud runs industry-leading information security operations that combine rigorous processes, expert incident response teams, and a multi-layered information security and privacy infrastructure. You can learn more about Google Cloud's data incident response process in the following resources: Google Cloud security whitepaper https://cloud.google.com/docs/security/overview/whitepaper Cloud-native security whitepaper https://cloud.google.com/security/beyondprod Infrastructure security design overview https://cloud.google.com/security/infrastructure/design/ Data incident response process https://cloud.google.com/security/incident-response	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
2.	The SLAs contain Google commitments regarding availability of the Service. They are available on the Google Cloud Platform Service Level Agreements and the Google Workspace Service Level Agreements pages. The Technical Support Services Guidelines describe our support response times. Google Cloud Platform Service Level Agreements https://cloud.google.com/terms/sla/ Google Workspace Service Level Agreements https://workspace.google.com/terms/sla.html Technical Support Services Guidelines https://cloud.google.com/terms/tssg	Services Technical Support
3.	Google Cloud will make available to Customer information about developments that adversely affect its ability to perform the Services in accordance with the SLA. More information is available on ourIncidents and the Google Cloud Service Health Dashboard and Google Workspace Status Dashboard pages. Incidents and the Google Cloud Service Health Dashboard https://cloud.google.com/support/docs/dashboard Google Workspace Status Dashboard https://www.google.com/appsstatus/dashboard/ In addition, Google Cloud will promptly and without unreasonable delay notify Customer of any Data Incident. More information about Google's data incident response process is available in our data incident response whitepaper. Data incident response process whitepaper https://services.google.com/fh/files/misc/data_incident_response_2018.pdf See below how Google CLoud investigates root causes. Data incident response process https://cloud.google.com/security/incident-response	-
4.	Information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide. Disaster Recovery Planning Guide https://cloud.google.com/architecture/dr-scenarios-planning-guide	-
4. (1)	For more information on security refer to 1.(2), 6).	-
4. (2)	For more information on data extraction refer to 1.(6), 3). The cost of migration is transparent and based on our publicly listed service fees. Our services enable you to transfer your data independently. However, if a regulated entity would like support, upon request, Google will provide advisory and implementation services to assist in migrating workloads or otherwise transitioning use of the Services subject to agreeing additional fees.	Transition Assistance

Control no.	Google Response	Google Cloud Financial Services Contract reference
C22	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google employees and contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new employees and contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.	-
C23	Google is ISO 27001 certified. This standard outlines "Supplier Relationships" (ISO 27001:2013, Annex A.15). Our information security administrative systems and vendor security initiatives, etc., have been reviewed and verified by a third party auditor, and we have obtained a SOC 2 Type 2 report. Google provides the following published information to help companies evaluate Google Cloud as an external provider. • The Google Security Whitepaper provides a comprehensive description of the various services available, as well as our systems for ensuring data security (protection of confidentiality) and integrity https://cloud.google.com/security/overview/whitepaper • Google can provide SOC audit reports through independent external auditors • On request, Google offers functionality for retrieving logs of instances in which Google Cloud accesses customer data. https://cloud.google.com/access-transparency • Customers can also refer to the following resources about our subprocessors: https://cloud.google.com/terms/subprocessors https://cloud.google.com/terms/data-processing-terms (section 11. Subprocessors)	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
C24	When evaluating Google as an external provider, security measures can be taken through the following information and agreements. • The Google Security Whitepaper allows you to comprehensively check the availability of various services, as well as our systems for ensuring data security (protection of confidentiality) and integrity: Google Cloud Security Whitepaper https://cloud.google.com/security/overview/whitepaper GoogleWorkspace Security Whitepaper https://static.googleusercontent.com/media/workspace.google.com/en//intl/ja/files/google-apps-security-and-compliance-whitepaper.pdf • Google can provide SOC audit and similar reports through independent auditors. • Customers have the right to control their own data, including personal data. Google provides security services to help protect customer data. • For information on compliance with regulations, check the official page below: Compliance resource center https://cloud.google.com/security/compliance To review our data processing terms and data incident response process, please refer to the following resources: Data Processing and Security Terms https://cloud.google.com/terms/data-processing-terms Data Incident Response Whitepaper https://cloud.google.com/docs/security/incident-response	-
C25	-	-
C26	-	-
C27	-	-
P1	-	-
P2	-	-
P3	-	-
P4	-	-
P5	-	-
P6	-	-
P7	-	-
P8	-	-
P9	-	-
P10	-	-
P11	-	-
P12	-	-
P13	-	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
P14	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Security Management" (ISO27001:2013, Annex A.13.1). We uses sophisticated data processing pipelines to integrate host-based signals on individual devices, network-based signals from various monitoring points in the infrastructure, and signals from infrastructure services. Rules and machine intelligence built on top of these pipelines give operational security engineers warnings of possible incidents. Our investigation and incident-response teams triage, investigate, and respond to these potential incidents 24 hours a day, 365 days a year. We conduct Red Team exercises to measure and improve the effectiveness of our detection and response mechanisms. We have 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. 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. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately. To review our data processing terms and data incident response process, please refer to the following resources: Data Processing and Security Terms https://cloud.google.com/terms/data-processing-terms/ Data Incident Response Whitepaper https://cloud.google.com/security/incident-response You can refer to the following resource to review how security is designed into Google's technical infrastructure. https://cloud.google.com/docs/security/infrastructure/design	-
P15	Google Cloud offers limited access points that can be accessed from external networks. Unnecessary communication ports and communication functions are blocked or restricted.	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
P16	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Security Management" (ISO27001:2013, Annex A.13.1). We uses sophisticated data processing pipelines to integrate host-based signals on individual devices, network-based signals from various monitoring points in the infrastructure, and signals from infrastructure services. Rules and machine intelligence built on top of these pipelines give operational security engineers warnings of possible incidents. Our investigation and incident-response teams triage, investigate, and respond to these potential incidents 24 hours a day, 365 days a year. We conduct Red Team exercises to measure and improve the effectiveness of our detection and response mechanisms. We have 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. 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. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately. To review our data processing terms and data incident response process, please refer to the following resources: Data Processing and Security Terms https://cloud.google.com/terms/data-processing-terms/ Data Incident Response Whitepaper https://cloud.google.com/security/incident-response You can refer to the following resource to review how security is designed into Google's technical infrastructure. https://cloud.google.com/docs/security/infrastructure/design	-
P17	-	-
P18	-	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
P19	Google is certified to the ISO27001 Standard, which regulates "Access to Networks and Network Services" (ISO27001:2013, Annex A.9.1.2), "Network Controls" (ISO27001:2013, Annex A.13.1.1). We have 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. 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. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment and ensure unauthorized access is detected and reviewed appropriately. To review our data processing terms and data incident response process, please refer to the followings: Data Processing and Security Terms https://cloud.google.com/terms/data-processing-terms/ Data Incident Response Whitepaper https://cloud.google.com/security/incident-response	-
P20	-	-
P21	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
P22	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (ISO27001:2013, Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity	-
P23	-	-
P24	-	-
P25	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Google employees have access to customer data. For Google employees, access rights and levels are based on their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	-
P26	-	-
P27	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google periodically reviews logical access to all systems to ensure appropriateness of access. Further, Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
P28	-	-
P29	-	-
P30	-	-
P31	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2). Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google employees and contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new employees and contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.	-
P32	Google is certified to the ISO27001 Standard, which regulates "Protection from Malware" (Annex A.12.2). Controls relating to vulnerability management are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google administers a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google also maintains relationships and interfaces with members of the security research community to track reported issues in Google services and open source tools. More information about reporting security issues can be found at https://www.google.com/about/appsecurity Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate protective measures against viruses.	-
P33	-	-
P34	-	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
P35	Google is ISO 27001 certified. This standard outlines "Access Control" (ISO 27001:2013, Annex A.9). Our information security administrative systems, including logical access control, have been reviewed and verified by a third party, and we have obtained a SOC 2 Type 2 report. Google employees' access rights and level of access are determined based on their roles and duties. Access rights are granted on the principle of least privilege and on a need-to-know basis, consistent with each employee's designated duties. Prior to joining our staff, Google will verify an individual's education, previous employment, and reference checks. Where local labor laws or statutory regulations permit, Google may also conduct criminal, credit, immigration, and security checks. The extent of these background checks is dependent on the desired position. Access by Google employees is monitored and audited by dedicated security, privacy, and internal audit teams. Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. Google also provides admin access logs in accordance with Google Cloud access transparency standards Access Transparency https://cloud.google.com/access-transparency	-
P36	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
P37	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. For Google employees, access rights and levels are based on an their job function and role, using the concepts of least–privilege and need–to–know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. These tools control both the modification of authorization settings and the approval process to ensure consistent application of the approval policies. An employee's authorization settings are used to control access to all resources, including data and systems for Google Cloud and Google Workspace products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. Googler access is monitored and audited by our dedicated security, privacy, and internal audit teams. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including developing guidance for access to operational documentation.	-
P38	Google is ISO 27001 certified. This standard outlines "Access Control" (ISO 27001:2013, Annex A.9). Our information security administrative systems, including logical access control, have been reviewed and verified by a third party, and we have obtained a SOC 2 Type 2 report. Operations carried out by Google employees are recorded and validated. Access is monitored and audited by dedicated security, privacy, and internal audit teams. Google also provides admin access logs in accordance with Google Cloud access transparency standards . Google Cloud customers bear all rights and responsibilities for the configuration and management of the environment they use. Google employees cannot operate systems that are managed by customers. Access Transparency https://cloud.google.com/access-transparency	-
P39	-	-
P40	-	-
P41	-	-
P42	-	-
P43	-	-
P44	Google has established a quality control system that meets best practice guidelines established by the International Organization for Standardization (ISO). The quality control system covers the operation of products containing assets that support the development and operation of Google Cloud and Google Workspace. Google's quality control system automates the steps, processes, resources, and other elements required for Google Cloud and Google Workspace quality control, and manages information appropriately.	-
P45	Google has established a quality control system that meets best practice guidelines established by the International Organization for Standardization (ISO). The quality control system covers the operation of products containing assets that support the development and operation of Google Cloud and Google Workspace. Google's quality control system automates the steps, processes, resources, and other elements required for Google Cloud and Google Workspace quality control, and manages information appropriately.	-
P46	-	-
P47	-	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
P48	Google is certified to the ISO27001 Standard, which regulates "Responsibility for Assets" (ISO 27001:2013, Annex A.8.1), "Disposal of Media" (ISO 27001:2013, Annex A.8.3.2), "Secure Disposal or Reuse of Equipment" (ISO 27001:2013, Annex A. 11.2.7) and "Control of Operational Software (ISO 27001:2013, Annex A.12.5.). Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction, via bar codes and asset tags. Metal detectors and video surveillance are implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing multiple step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment.	-
P49	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security whitepaper : State-of-the-art data centers https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google Workspace Security whitepaper https://static.googleusercontent.com/media/workspace.google.com/en//intl/ja/files/google-apps-security-and-compliance-whitepaper.pdf Google Data Center Security: 6 Layers Deep https://www.youtube.com/watch?v=kd33UVZhnAA	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
P50	Google is certified to the ISO27001 Standard, which regulates "Equipment" (ISO 27001:2013, Annex A.11.2). Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security whitepaper : State-of-the-art data centers https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google Workspace Security whitepaper https://static.googleusercontent.com/media/workspace.google.com/en//intl/ja/files/google-apps-security-and-compliance-whitepaper.pdf Google Data Center Security: 6 Layers Deep https://www.youtube.com/watch?v=kd33UVZhnAA	-
P51	Google is certified to the ISO27001 Standard, which regulates "Equipment Maintenance" (ISO 27001:2013, Annex A.11.2.4).	-
P52	Google is certified to the ISO27001 Standard, which regulates "Equipment Maintenance" (ISO 27001:2013, Annex A.11.2.4).	-
P53	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security whitepaper : State-of-the-art data centers https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google Workspace Security whitepaper https://static.googleusercontent.com/media/workspace.google.com/en//intl/ja/files/google-apps-security-and-compliance-whitepaper.pdf Google Data Center Security: 6 Layers Deep https://www.youtube.com/watch?v=kd33UVZhnAA	-
P54	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report.	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
P55	Google is certified to the ISO27001 Standard, which regulates "Capacity Management" (ISO 27001:2013, Annex A.12.1.3). Google has a robust network that monitors and adjusts capacity on an as-needed basis worldwide.	-
P56	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security whitepaper : State-of-the-art data centers https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google Workspace Security whitepaper https://static.googleusercontent.com/media/workspace.google.com/en//intl/ja/files/google-apps-security-and-compliance-whitepaper.pdf Google Data Center Security: 6 Layers Deep https://www.youtube.com/watch?v=kd33UVZhnAA	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
P57	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security whitepaper : State-of-the-art data centers https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google Workspace Security whitepaper https://static.googleusercontent.com/media/workspace.google.com/en//intl/ja/files/google-apps-security-and-compliance-whitepaper.pdf Google Data Center Security: 6 Layers Deep https://www.youtube.com/watch?v=kd33UVZhnAA	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
P58	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored and logged. To learn more about our Data Center Processes, please see our Security Whitepaper and Data Center Introduction videos: Google Security whitepaper : State-of-the-art data centers https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google Workspace Security whitepaper https://static.googleusercontent.com/media/workspace.google.com/en//intl/ja/files/google-apps-security-and-compliance-whitepaper.pdf Google Data Center Security: 6 Layers Deep https://www.youtube.com/watch?v=kd33UVZhnAA	-
P59	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored, logged and periodically approved for appropriateness. Employees with access must follow documented policies and procedures for the type of secured areas they are working in.	-
P60	Google is certified to the ISO27001 Standard, which regulates "Physical and Environmental Security" (ISO27001:2013, Annex A.11) and "Equipment Maintenance" (ISO 27001:2013, Annex A.11.2.4). Physical controls relating to availability of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Physical access to secured areas (such as the data server floor) is only possible via a security corridor. Google implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter secured areas, and all access to those area is monitored, logged and periodically approved for appropriateness. Employees with access must follow documented policies and procedures for the type of secured areas they are working in.	-
P61	-	-
P62	-	-
P63	-	-
P64	-	-
P65	-	-
P66	-	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
P67	-	-
P68	-	-
P69	You can refer to the following docs to review service for protection of customer data. Sensitive Data Protection https://cloud.google.com/dlp/docs	-
P70	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2), and "Backup" (ISO27001:2013 Annex A 12.3.), and "Documented Operating Procedures" (ISO27001:2013, Annex A 12.1.1). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Google Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters. The Google Cloud Service Health Dashboard provides status information on services that are part of Google Cloud. Status can include service disruptions, outages, or informational messages about a temporary issue. The Google Workspace Status Dashboard provides information on the current status of core Google Workspace services, such as Gmail, Google Calendar, and Google Meet. The dashboards shows the current status for each service, and any recent outages or disruptions. Click on a notification icon for more information about the issue, including an estimate of when it might be resolved The global Customer Care team monitors the status of services using many different types of signals and updates the dashboard in the event of a widespread issue. If needed, they will post a detailed incident analysis report after an incident has been resolved. Incidents and the Google Cloud Service Health Dashboard https://cloud.google.com/support/docs/dashboard Data Incident Response Whitepaper https://cloud.google.com/security/incident-response	-
P71	-	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
P72	Google provides customers with information on any developments that may adversely impact our ability to operate these services in accordance with the relevant service level agreements. More information is available on our Incidents and the Google Cloud Service Health Dashboard page. Incidents and the Google Cloud Status Dashboard https://cloud.google.com/support/docs/dashboard Google also notifies customers of any data incidents quickly and without unreasonable delay. More information on Google's data incident response process can be found in our Data Incident Response Whitepaper. Data Incident Response Whitepaper https://services.google.com/fh/files/misc/data_incident_response_2018.pdf To review how Goolge investigate the root cause, please refer to the following: https://cloud.google.com/security/incident-response	-
P73	-	-
P74	-	-
P75	-	-
P76	-	-
P77	-	-
P78	-	-
P79	-	-
P80	-	-
P81	-	-
P82	-	-
P83	-	-
P84	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Google Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
P85	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Google Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	-
P86	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Google Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
P87	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Google Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	-
P88	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Google Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including configuring appropriate regions and zones to prevent failures or disasters.	-
P89	-	-
P90	-	-
P91	-	-
P92	-	-
P93	-	-
P94	-	-
P95	-	-
P96	-	-
P97	-	-
P98	-	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
P99	-	-
P100	Google is certified to the ISO27001 Standard, which regulates "System Acquisition, Development and Maintenance" (ISO27001:2013, Annex A.14). Please see the Google Infrastructure Security Design Overview for more details. Google Infrastructure Security Design Overview https://cloud.google.com/security/security-design/ Customers using Google Cloud retain all rights and responsibilities to configure and manage their environment, including system development procedures.	-
P101		-
P102	Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A.12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs.	-
P103	Google is certified to the ISO27001 Standard, which regulates "Logging and Monitoring" (ISO 27001:2013, Annex A.12.4). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs.	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
P103-1	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Google Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions. Customers have to take the necessary measures to ensure that redundancy and backup configurations work properly. You can leverage the redundancy and backup features provided by each service.	-
P104	Google is certified to the ISO27001 Standard, which regulates "Redundancies" (ISO27001:2013, Annex A.17.2). Controls relating to availability and integrity of systems are also reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and internet connectivity, and the software services themselves. This “redundancy of everything” includes the handling of errors by design and creates a solution that is not dependant on a single server, data center, or network connection. Google’s data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that Google Cloud and Google Workspace customers can continue working in most cases without interruption. Google’s highly redundant infrastructure also helps protect our customers from data loss. For Google Cloud Products (Google Workspace and Google Cloud), our Recovery Point Objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Cloud products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions.	-
P105	-	-
P106	-	-
P107	-	-
P108	-	-
P109	-	-
P110	-	-
P111	-	-
P112	-	-
P113	-	-
P114	-	-
P115	-	-
P116	-	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
P117	-	-
P118	-	-
P119	-	-
P120	-	-
P121	-	-
P122	-	-
P123	-	-
P124	-	-
P125	-	-
P126	-	-
P127	-	-
P128	-	-
P129	-	-
P130	-	-
P131	-	-
P132	-	-
P133	-	-
P134	-	-
P135	-	-
P136	-	-
P137	-	-
P138	-	-
P139	-	-
P140	-	-
P141	-	-
P142	-	-
P143	-	-
P144	-	-
P145	-	-
P146	-	-
P147	-	-
P148	-	-
F1	Google locates its data centers in areas that are not prone to various disasters.	-
F2	At Google data centers, we regularly conduct environmental inspections and take appropriate disaster measures.	-
F3	Google meets legal building and facility requirements for the regions in which its data centers are located.	-
F4	Google meets legal building and facility requirements for the regions in which its data centers are located.	-
F5	Google data centers feature a multi-layered physical security model with safeguards such as alarms, vehicle access barriers, and perimeter fencing.	-
F6	There are no signs indicating location of Google data centers.	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
F7	Google data centers have appropriate lightning protection systems and ground connections. The lightning protection systems in place are in accordance with the Building Standards Act and other relevant laws.	-
F8	Google data centers are separated into sections and include safeguards such as custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics. Access is granted only to approved employees with specific roles to enter.	-
F9	Google data centers use underground cables and non-combustible materials to prevent severing and spread of fire.	-
F10	Google meets legal building and facility requirements for the regions in which its data centers are located.	-
F11	Google meets legal building and facility requirements for the regions in which its data centers are located.	-
F12	Google meets legal building and facility requirements for the regions in which its data centers are located.	-
F13	Google data centers are protected by robust perimeter walls, etc.	-
F14	Google's data centers take measures to prevent the spread of fire in accordance with national and regional fire and fire prevention standards.	-
F15	Google data centers are equipped with alarmed security systems.	-
F16	Google's data centers have one entrance and exit that is used at all times, and we have implemented security measures such as security guards, contactless card entry, and the installation of surveillance cameras.	-
F17	Google data centers are equipped with emergency exits and place high importance on employee safety. Appropriate signage has been installed and training is carried out to ensure all staff can safely evacuate in the event of an emergency.	-
F18	Google's data centers take appropriate flood countermeasures based on an assessment of the environmental risks in the area.	-
F19	Robust, lockable doors are used at the entrances to Google data centers.	-
F20	Google meets legal building and facility requirements for the regions in which its data centers are located.	-
F21	Google data centers are designed to prevent collapse or damage during earthquakes.	-
F22	Google meets building and facility requirements for the regions in which its data centers are located, and operates facilities in line with best practices to limit damage to the greatest possible extent in the event of natural disasters. JQA-compliant server spaces are located above base isolation layers.	-
F23	Access to secure areas (e.g. server spaces) is only possible via security corridors. These security corridors implement multi-factor access control using security badges and biometrics. Access is granted only to approved employees with specific roles to enter. Access to these areas is monitored and recorded, and access privileges are periodically reviewed.	-
F24	Google room names are not displayed outside spaces leased from colocation providers. Colocation providers maintain fire-prevention floor plans and store them in locations inaccessible to third parties.	-
F25	Google data center server spaces are spacious enough for the operation and maintenance of equipment, and have safe evacuation routes in place. There is enough space to open and close doors without moving equipment.	-
F26	Google data center server spaces are in separate, dedicated zones.	-
F27	Server space in Google's data centers is limited to one entrance that is used at all times, and if the entrance door is left open for an extended period of time, an alarm will be activated and the monitoring center will be notified. Additionally, we have a policy prohibiting tailgating, and entrances and exits are monitored 24 hours a day remotely.	-
F28	Robust, lockable doors are used at the entrances to Google data center server spaces.	-
F29	All server spaces in Google data centers are windowless.	-
F30	Google data center server spaces have two way emergency exit routes, and high importance is placed on employee safety; appropriate signage has been installed and training is carried out to ensure all staff can safely evacuate in an emergency.	-
F31	Google data center server spaces are in separate, fireproof blocks in compliance with the Building Standards Act.	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
F32	Google data center server spaces are equipped with water leakage sensors. If the sensors are triggered, alerts are activated in the affected zone and DC operations control room.	-
F33	Google data centers continuously engage in ESD programs featuring guidance on ESD prevention. (ESD: Electrostatic discharge)	-
F34	Google data center server space interiors are made with non-flammable, fireproof materials.	-
F35	Google meets building requirements for the regions in which its data centers are located, and operates facilities in line with best practices to limit damage to the greatest possible extent in the event of natural disasters. Interiors, etc. are designed to prevent collapse or damage during earthquakes.	-
F36	The free access floor for server space in Google's data centers meets the earthquake risk and earthquake resistance standards of each country and region.	-
F37	Google data center facilities are equipped with robust fire-extinguishing equipment and comprehensive safeguards to detect and prevent fire. Fire detectors and extinguishers are in place to prevent damage to hardware. If a heat, fire, or smoke detector is triggered, alarms are activated simultaneously in the affected zone and DC operations control room.	-
F38	If a heat, fire, or smoke detector in a Google data center is triggered, alerts are activated simultaneously in the affected zone and DC operations control room.	-
F39	Google data center facilities are equipped with robust fire-extinguishing equipment and comprehensive safeguards to detect and prevent fire. Fire detectors and extinguishers are in place to prevent damage to hardware. If a heat, fire, or smoke detector is triggered, alarms are activated simultaneously in the affected zone and DC operations control room.	-
F40	Fire spread prevention measures have been taken to prevent the spread of fire at the penetrations from other sections of the server space at Google's data center.	-
F41	Google meets legal building and facility requirements for the regions in which its data centers are located.	-
F42	Google data center server spaces are equipped with emergency and portable lighting.	-
F43	Google data center server spaces are free from water-related facilities.	-
F44	At Google's data centers, they have installed and implemented appropriate measures based on disaster predictions in each region. For example, as part of our response standards in the event of an earthquake, they have installed earthquake detectors to measure the seismic intensity inside the building.	-
F45	Access to Google data center secure areas (e.g. server spaces) is possible, multidimensional access control using security badges and biometric authentication is required. In addition, access is granted to approved employees with specific roles to enter, which is regularly reviewed. An alarm is activated and a response system is in place.	-
F46	Environmental health and safety controls are enforced across Google data centers, and facilities implement adequate environmental safeguards in place. Temperature and humidity measurement and alarm devices are installed in appropriate locations and constantly monitored.	-
F47	Google meets building and facility requirements for the regions in which its data centers are located. In accordance with management standards for environmental sanitation in buildings as prescribed in the Act on Maintenance of Sanitation in Buildings, appropriate precautions are taken with regard to operation and maintenance, patrols, etc. There are also no kitchen or restaurant facilities inside the buildings.	-
F48	Appliances and equipment in Google data center server spaces are made with non-flammable materials.	-
F49	Environmental health and safety controls are enforced across Google data centers, and facilities implement comprehensive environmental safeguards. In addition to training on applicable standards, we continuously engage in ESD programs involving ESD prevention at all of our data centers. (ESD: Electrostatic discharge).	-
F50	Google meets building and facility requirements for the regions in which its data centers are located, and operates facilities in line with best practices to limit damage to the greatest possible extent in the event of natural disasters. Equipment is fitted with safeguards against earthquakes.	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
F51	Carts (i.e. hand trucks) are permitted in Google data center server spaces to transport items in and out. They are not left inside the server spaces. All carts are equipped with locking mechanisms.	-
F52	Google meets building and facility requirements for the regions in which its data centers are located, and designs and constructs the data centers in line with best practices to limit damage to the greatest possible extent in the event of natural disasters.	-
F53	Google data center power and air-conditioning equipment rooms are spacious enough to operate and maintain equipment, and have safe evacuation routes in place. There is enough space to open and close doors without moving equipment.	-
F54	Google data centers have dedicated rooms for power and air-conditioning equipment. Access to power and air-conditioning equipment rooms is only granted to personnel who require entry for essential work purposes.	-
F55	Google power and air-conditioning equipment rooms are windowless and have robust, lockable doors specifically designed to stop the spread of fire. Power and air-conditioning equipment rooms have one entrance.	-
F56	Environmental health and safety controls are enforced across Google data centers, and facilities implement comprehensive environmental safeguards. Power and air-conditioning equipment rooms are equipped with robust fire-extinguishing equipment and comprehensive safeguards to detect and prevent fire.	-
F57	Environmental health and safety controls are enforced across Google data centers, and facilities implement comprehensive environmental safeguards. Power and air-conditioning equipment rooms are equipped with robust fire-extinguishing equipment and comprehensive safeguards to detect and prevent fire. Fire detectors and extinguishers are in place to prevent damage to hardware. If a heat, fire, or smoke detector in a Google data center is triggered, alerts are activated simultaneously in the affected zone and DC operations control room.	-
F58	Environmental health and safety controls are enforced across Google data centers, and facilities implement adequate environmental safeguards in place. Power and air-conditioning equipment rooms are equipped with robust fire-extinguishing equipment and comprehensive safeguards to detect and prevent fire. Google data center power and air-conditioning equipment rooms are equipped with gas-based fire-extinguishing equipment. Additionally, fire extinguishers are placed in appropriate locations based on the fire regulations of each region.	-
F59	Google meets legal building and facility requirements for the regions in which its data centers are located.	-
~~F60~~	Google data center power and air-conditioning equipment rooms use cable ducts made of non-combustible materials and other safeguards to prevent the spread of fire.	-
F61	Google data center power facilities are designed and built with fail-safes.	-
F62	Google data centers are in operation 24 hours a day, with redundant power supplies and environmental management ensuring uninterrupted service. All critical components are equipped with main and alternative power sources supplying the same amount of power.	-
F63	Google data centers use uninterruptible power supply (UPS) systems to ensure stable operation of computer systems. In addition, through the use of backup generators, there is power to maintain maximum performance even in the event of an emergency.	-
F64	Google meets legal building and facility requirements for the regions in which its data centers are located.	-
F65	Google data centers are equipped with lightning arresters to prevent surges from grounding electrodes, and surge protection devices (SPDs) to discharge induced surges.	-
F66	Google meets building and facility requirements for the regions in which its data centers are located, and operates facilities in line with best practices to limit damage to the greatest possible extent in the event of natural disasters. Equipment is fitted with safeguards against earthquakes.	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
F67	Google server spaces use dedicated circuits. Multiple power systems supply server spaces, and the power is routed through the facility appropriately.	-
F68	In Google server spaces, devices that may cause significant load fluctuations do not share the same power source.	-
F69	Google data centers use dedicated grounding for computer systems.	-
F70	In Google data centers, power supplies are wired from breakers and current leakage alarms are installed to protect each device from overcurrent.	-
F71	Google data centers use UPS power systems as a safeguard against disasters and criminal activity. In addition, through the use of backup generators, there is power to maintain maximum performance even in the event of an emergency.	-
F72	Google data center air-conditioning units are designed and built with fail-safes. The operating temperature of servers and other hardware is maintained at a fixed level, reducing the risk of service interruptions.	-
F73	Google installs and maintains cooling systems in accordance with industry best practices. Automatic controllers and anomaly alarms are installed, and the humidity and temperature of computer rooms are monitored, managed and appropriately adjusted.	-
F74	Google data centers use dedicated air-conditioning units for computer rooms.	-
F75	Google data centers are in operation 24 hours a day, with fail-safe redundancy systems, automatic controllers, and anomaly alarms ensuring uninterrupted service. Google installs and maintains cooling systems in accordance with industry best practices.	-
F76	Google data centers are in operation 24 hours a day, with fail-safe redundancy systems, automatic controllers, and anomaly alarms ensuring uninterrupted service. Google installs and maintains cooling systems in accordance with industry best practices.	-
F77	Google data centers have dedicated rooms for power and air-conditioning equipment. Access to power and air-conditioning equipment rooms is granted only to personnel who require entry for essential work purposes.	-
F78	Google meets building and facility requirements for the regions in which its data centers are located, and operates facilities in line with best practices to limit damage to the greatest possible extent in the event of natural disasters. Equipment is fitted with safeguards against earthquakes.	-
F79	Google data centers use non-combustible materials for thermal insulation systems and air-conditioning unit vents to prevent damage in the event of a fire.	-
F80	Google data centers are equipped with central monitoring systems and surveillance equipment, etc. In the event of a failure or abnormality, the system immediately issues an alarm and responds accordingly.	-
F81	Google data centers are equipped with central monitoring systems and surveillance equipment, etc. In the event of a failure or abnormality, the system immediately issues an alarm and responds accordingly.	-
F82	In Google's data centers, circuit-related facilities are securely locked, and access is granted to personnel who require entry for essential work purposes. The doors to circuit-related facilities do not indicate the nature of the room.	-
F83	In Google's data centers, circuit-related facilities are securely locked, and access is granted to personnel who require entry for essential work purposes. The doors to circuit-related facilities do not indicate the nature of the room.	-
F83-1	In Google's data centers, lines are routed through dedicated circuits to prevent failures and unauthorized access.	-
F84	-	-
F85	-	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
F86	-	-
F87	-	-
F88	-	-
F89	-	-
F90	-	-
F91	-	-
F92	-	-
F93	-	-
~~F94~~	-	-
F95	-	-
F96	-	-
F97	-	-
F98	-	-
F99	-	-
F100	-	-
F101	-	-
F102	-	-
F103	-	-
F104	-	-
F105	-	-
F106	-	-
F107	-	-
F108	-	-
F109	-	-
F110	-	-
F111	-	-
F112	-	-
F113	-	-
F114	-	-
F115	-	-
F116	-	-
F117	-	-
F118	-	-
F119	-	-
F120	-	-
F121	-	-
F122	-	-
F123	-	-
F124	-	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
F125	-	-
F126	-	-
F127	-	-
F128	-	-
F129	-	-
F130	-	-
F131	-	-
F132	-	-
F133	-	-
F134	-	-
F135	-	-
F136	-	-
F137	-	-
A1	-	-
A1-1	Google has an internal audit function to assess management compliance with Google ID, source code, and infrastructure management policies. Our internal audit function works with third-party organizations on a regular basis to independently review the effectiveness of the company's approach to information security management. In order to reduce impact internally and to customers, we plan and coordinate system security audits with relevant stakeholders in advance.	-
A1-2	-	-
A1-3	Google has an internal audit function to assess management compliance with Google ID, source code, and infrastructure management policies. Our internal audit function works with third-party organizations on a regular basis to independently review the effectiveness of the company's approach to information security management. In order to reduce impact internally and to customers, we plan and coordinate system security audits with relevant stakeholders in advance.	-
A1-4	Google has an internal audit function to assess management compliance with Google ID, source code, and infrastructure management policies. Our internal audit function works with third-party organizations on a regular basis to independently review the effectiveness of the company's approach to information security management. In order to reduce impact internally and to customers, we plan and coordinate system security audits with relevant stakeholders in advance.	-

Control no.	Google Response	Google Cloud Financial Services Contract reference
A1-5	Google is certified to the ISO27001 Standard, which regulates "Information Security Awareness, Education and Training" (ISO 27001:2013, Annex A.7.2.2), Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. All Google contractors undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new contractors agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more. Google may accept data cetenter or/and office audits from finantial institutions who have contracts with Google Cloud. Please Contact your Google Cloud sales representative for more information.	-