Korean FSC - IT Outsourcing Regulations

Google Workspace Mapping

This document is designed to help institutions supervised by the Korean Financial Services Commission ("**regulated entity**") to consider the [Regulation on Outsourcing of Information Processing Business of Financial Institutions](#) (the "**framework**") in the context of Google Workspace and the Google Cloud Financial Services Contract.

We focus on appendix 3 (outsourcing operation standards) of the framework. For each paragraph, we provide commentary to help you understand how you can address the requirements using the Google Cloud services and the Google Cloud Financial Services Contract.

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
1.	Regulated entities shall establish and operate outsourcing operation standards based on the following:		
2.	1. Risk assessment and management measures for outsourcing	Google recognizes that you need to conduct due diligence and perform a risk assessment before deciding to use our services. To assist you, we've provided information for some of the areas you may need to consider below. ● Qualifications and competencies: Google Cloud has been named as a leader in several reports by third party industry analysts. You can read these on our [Analyst Reports](#) page. ● Customer references: Information about our referenceable customers (including in the financial services sector) is available on our [Google Workspace Cloud Customer](#) page. ● Principals: Information about Google Cloud's leadership team is available on our [Media Resources](#) page. We also recognize 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 27001:2013 (Information Security Management Systems)](#) ● [ISO/IEC 27017:2015 (Cloud Security)](#) ● [ISO/IEC 27018:2014 (Cloud Privacy)](#) ● [SOC 1](#) ● [SOC 2](#) You can review Google's current [certifications and audit reports](#) at any time.	N/A Certifications and Audit Reports
3.	2. Termination and subcontracting of outsourcing contracts	Termination You can elect to terminate our contract for convenience with advance notice, including if necessary to comply with law or if directed by a supervisory authority. Subcontracting To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will:	Termination for Convenience Google Subcontractors

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		● 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 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).	
4.	3. Monitoring of outsourced task		
5.	Monitoring procedures for major issues related to outsourcing (service provider's financial status and risks, emergency plans and results, etc.), appointment of monitoring staff, and reporting system for management.	Service delivery You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: ● The Status Dashboard provides status information on the Services. ● Admin Console Reports allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. ● Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your user content. 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). Risks and emergencies 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 Status Dashboard page.	Ongoing Performance Monitoring Significant Developments

Korean FSC- IT Outsourcing Regulations

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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. Google's financial status You can review information about Google's financial status on Alphabet's Investor Relations page.	Data Incidents (Cloud Data Processing Addendum)
6.	4. Protection of customer data		
7.	Management of customer data;	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. You can provide Google instructions about your data and Google will comply with those instructions. Regulated entities can use the following functionality to control the Services: ● Admin Console: A web-based graphical user interface that customers can use to manage their Google Workspace resources. For more information about managing the security of customer data refer to Row 20.	Protection of Customer Data Google's Compliance with Instructions (Cloud Data Processing Addendum)
8.	Granting access only to authorized persons; and	Google recognizes that you need visibility into who did what, when, and where for all user activity on our service. Admin Console Reports allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. In particular, Google Workspace Audit Logs help your security teams maintain audit trails in Google Workspace and view detailed information about Admin activity, data access, and system events.	N/A
9.	Right to take action by customers in case of violation of confidentiality protection	Regulated entities may terminate our contract with advance notice for Google's material breach after a cure period.	Term and Termination
10.	5. Emergency plan		
11.	In case of contingency such as bankruptcy of service provider or communication problem	Google will implement a disaster recovery and business contingency plan for our 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.	Business Continuity and Disaster Recovery

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Information on the reliability of the Services is available on our Google Cloud Help page.	
12.	6.Securing access to outsourcing information		
13.	Ensure access to data by supervisory authorities or internal and external auditors	Regulated entities may access their data on the services at any time and may provide their supervisory authority with access.	Regulator Information, Audit and Access Customer Information, Audit and Access
14.	7. A financial institution's outsourcing agreement shall specify the following:		
15.	● The scope of outsourcing (provision cycle, contents and method), means of doing task	The Google Workspace services are described on our services summary page. You decide which services to use, how to use them and for what purpose. Therefore, you decide the scope of the arrangement.	Definitions
16.	● Provision of information (including key business information for service providers)	Refer to Row 5 for the information that we make available to you.	N/A
17.	● Audit on service provider	Refer to Row 1 for more information on the independent audits that Google undergoes for the Services In addition, Google recognizes that regulated entities must be able to audit our services effectively. Google grants audit, access and information rights to regulated entities and both their appointees.	Customer Information, Audit and Access
18.	● Fees and compensation for outsourcing	Refer to your Google Cloud Financial Services Contract.	Payment Terms
19.	● Regulated entities' ownership of outsourced data, Use of financial companies' physical facilities and intellectual property rights	Outsourced data and intellectual property. You retain all intellectual property rights in your data, the data you derive from your data using our services and your applications. Physical facilities Google doesn't make use of your physical facilities to deliver our services.	Intellectual Property N/A
20.	● Protection and confidentiality of customer data	The security and confidentiality of information when using a cloud service consists of two key elements: (1) 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.	Data Security; Security Measures (Cloud Data Processing Addendum)

Korean FSC- IT Outsourcing Regulations

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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 (2) 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 certain data while it is stored at rest on a disk (including solid-state drives) or backup media. Even if an attacker or someone with physical access obtains the storage equipment containing your data, they won't be able to read it because they don't have the necessary encryption keys. • **Encryption in transit.** Google encrypts all data while it is "in transit"--traveling over the Internet and across the Google network between data centers. Should an attacker intercept such transmissions, they will only be able to capture encrypted data, at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. (b) Security products	

Korean FSC- IT Outsourcing Regulations

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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	
21.	● Emergency plans such as securing a backup system to ensure business continuity	Refer to Row 11 for information about Google's business continuity plans and how customers can use our Services in their own business continuity planning. In addition, regulated entities can use Spinbackup as part of their backup routine. Refer to our solutions page for more information about how you can configure Spinbackup Google Workspace backup and restore your Google Workspace data.	N/A
22.	● Indemnification, insurance, dispute resolution (mediation, arbitration, etc.)	Indemnification Refer to your Google Cloud Financial Services Contract. Insurance Google will maintain insurance cover against a number of identified risks. Despite Resolution Refer to your Google Cloud Financial Services Contract.	Indemnification Insurance Governing Law
23.	● Service Provider Liability Limitations	Refer to your Google Cloud Financial Services Contract.	Liability
24.	● Termination of contract (regulated entities' right to terminate the contract, return of data, etc.)	Termination You can elect to terminate our contract for convenience with advance notice, including if necessary to comply with law or if directed by a supervisory authority.	Term and Termination

Google Cloud

Korean FSC- IT Outsourcing Regulations

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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.	
		Return of data	Transition Term
		Google recognizes 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 the transition term. More information is available on our Google Account help page.	
		In addition, Data Export is a feature that makes it easy to export and download a copy of your data securely from our Services.	Data Export (Cloud Data Processing Addendum)
		Deletion	
		On termination of the contractual relationship, Google will comply with your instruction to delete Customer Data from Google systems.	Deletion on Termination (Cloud Data Processing Addendum)
25.	● Audits by supervisory authority	Google grants audit, access and information rights to regulated entities and supervisory authorities, and both their appointees.	Regulator Information, Audit and Access
26.	● Service provider's joint liability for damages caused by subcontracting	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 and will remain liable to you for any subcontracted obligations.	Subcontracting; Google Subcontractors
27.	● Service provider's responsibility for subcontracting	Google will remain responsible for the performance of all subcontracted obligations. Refer to Row 3 for the conditions that Google will comply with for subcontracting.	Google Subcontractors
28.	● Governing law and competent court (if the service provider is located in a foreign country)	Refer to your Google Cloud Financial Services Contract.	Governing Law