MAS Notice 655 Cyber Hygiene

Google Workspace Mapping

This document is designed to help financial institutions (“**regulated entity**”) supervised by the Monetary Authority of Singapore (“**MAS**”) to consider Notice 655 Cyber Hygiene (“**framework**”) in the context of Google Workspace and the Google Cloud Services Contract.

We focus on the following requirements of the framework: IV. Cyber Hygiene Practices. 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 Services Contract.

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
1	**4.1 Administrative Accounts**		
2	A relevant entity must ensure that every administrative account in respect of any operating system, database, application, security appliance or network device, is secured to prevent any unauthorised access to or use of such account.	This is a shared responsibility between Google and the customer. Different platforms have different shared responsibilities. Within customer organizations, administrative roles and privileges for Google Workspace are configured and controlled by the administrator owner. This means that individual team members can manage certain services or perform specific administrative functions without gaining access to all settings and data. For it’s part, Google takes appropriate measures to manage administrative accounts with BeyondCorp. BeyondCorp is used by most Googlers every day to provide user- and device-based authentication and authorization for Google's core infrastructure and corporate resources. BeyondCorp is Google's implementation of the zero trust model. It builds upon a decade of experience at Google, combined with ideas and best practices from the community. By shifting access controls from the network perimeter to individual users, BeyondCorp enables secure work from virtually any location without the need for a traditional VPN. Google enables you to protect and manage your Google Workspace admin accounts through the services offered. For example: • 2-Step Verification assists with preventing unauthorized access to administrative accounts. It’s especially important for super admins to use 2SV because their accounts control access to all business and employee data in the organization. • Admin Audit Log is a feature to see a record of actions performed in your Google Admin console. For example, you can see when an administrator added a user or turned on a Google Workspace service. • Cloud Identity is a unified identity, access, app, and endpoint management (IAM/EMM) platform that helps IT and security teams maximize end-user efficiency and protect your organization’s data.	Data Security (Data Processing Amendment)
3	**4.2 Security Patches**		
4	(a) A relevant entity must ensure that security patches are applied to address vulnerabilities to every system, and apply such security patches within a timeframe that is commensurate with the risks posed by each vulnerability.	Security patching is a shared responsibility between Google and the customer. Different platforms have different shared responsibilities. More information is available at: • Our Security patching page	Security Measures (Data Processing Amendment)

		• Our OS Patch Management page Additionally, 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 security whitepaper	
5	(b) Where no security patch is available to address a vulnerability, the relevant entity must ensure that controls are instituted to reduce any risk posed by such vulnerability to such a system.	Google recognizes that entities need to review our internal controls as part of their risk assessment. To assist, Google undergoes several independent third-party audits on at least an annual basis to provide independent verification of our operations and internal controls. 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 • SOC 3 You can review Google's current certifications and audit reports at any time.	Audited Services (Data Processing Amendment)
6	**4.3 Security Standards**		
7	(a) A relevant entity must ensure that there is a written set of security standards for every system.	This is a customer consideration. Refer to Row 5 for information on the system security standards that Google complies with.	N/A
8	(b) Subject to sub-paragraph (c), a relevant entity must ensure that every system conforms to the set of security standards.	N/A	N/A
9	(c) Where the system is unable to conform to the set of security standards, the relevant entity must ensure that controls are instituted to reduce any risk posed by such non-conformity.	This is a customer consideration. Refer to Row 5 for information on the system security standards that Google complies with.	N/A
10	**4.4 Network Perimeter Defence**		
11	A relevant entity must implement controls at its network perimeter to restrict all unauthorised network traffic.	This is a customer consideration. Google provides our customers with the ability to set up and configure their network to restrict unauthorized network traffic. More information is available at: • Google Workspace Admin Network Help details that you can have the device automatically try to connect to a secure network with username or identity credentials specified by policy. Additionally, refer to Row 5 for information on the system controls and security standards that Google complies with.	Audited Services (Data Processing Amendment)
12	**4.5 Malware protection**		

13	A relevant entity must ensure that one or more malware protection measures are implemented on every system, to mitigate the risk of malware infection, where such malware protection measures are available and can be implemented.	This is a customer consideration. Google offers services to assist our customers with malware protection measures. For example: ● With Google Workspace Security Dashboard you can use the security dashboard to see an overview of different security reports, such as Malware reports. ● Advanced phishing and malware protection - As an administrator, you can protect incoming mail against phishing and harmful software (malware). You can also choose what action to take based on the type of threat detected. ● Set up rules to detect harmful attachments - Gmail can scan or run attachments in a virtual environment called Security Sandbox. Attachments identified as threats are sent to the recipient's Spam folder. For more information, refer to our security whitepaper.	N/A
14	**4.6 Multi-factor Authentication**		
15	Subject to paragraph 4.7, a relevant entity must ensure that multi-factor authentication is implemented for the following:		
16	(a) all administrative accounts in respect of any operating system, database, application, security appliance or network device that is a critical system; and	This is a shared responsibility between Google and the customer. Different platforms have different shared responsibilities. Customers are responsible for implementing and operating multi-factor authentication measures used to determine and ensure the security of their data and applications in the cloud. Additionally, Google provides customers the capability to enable MFA. Customers can protect their user accounts and company data with a wide variety of MFA verification methods such as push notifications, Google Authenticator, phishing-resistant Titan Security Keys, and using your Android or iOS device as a security key. Refer here for more information. For it's part, Google requires MFA for employees to authenticate with their account to all Google corporate services by default. Lastly, refer to Row 2 for more information on administrator account security.	N/A
17	(b) all accounts on any system used by the relevant entity to access customer information through the internet.	This is a customer consideration. Refer to Row 16 for more information.	