REGULATION OF THE PRESIDENT OF THE REPUBLIC OF INDONESIA NUMBER 95 OF 2018

Google Cloud Mapping

This document is designed to help customers regulated by Republic of Indonesia to consider the President of the Republic of Indonesia Number 95 of 2018 about Electronic based Government System (**"GR 95"**) in the context of Google Cloud Platform (**"GCP"**).

We focus on Articles 40, 41, 46, 47, 48, 49, 50, 55, 56 and 58 of the framework. For each requirement, we provide commentary to help you understand how you can address the requirements using the Google Cloud services and controls

#	Presidential Regulation concerning Electronic-based Government System	Google Cloud Commentary
1.	**Article 40**	
	(1) SPBE security includes guarantee of confidentiality, integrity availability, authenticity and nonrepudiation of resources related to data and information, SPBE infrastructure, and SPBE Application.	Security The confidentiality and integrity of a cloud service consists of two key elements: 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 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 27001:2013 (Information Security Management Systems) • ISO/IEC 27017:2015 (Cloud Security) • ISO/IEC 27018:2014 (Cloud Privacy) • PCI DSS • SOC 1 • SOC 2 • SOC 3
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 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 **Use of your information** You can provide Google instructions about your data and Google will comply with those instructions. 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. **Privacy and NonPublic Personal Information** The Cloud Data Processing Addendum address the roles and responsibilities of the parties for your data. In particular, Google will: • comply with privacy laws and regulations applicable to it in the provision of the Services. • 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. • enable you to delete your information and comply with your instruction to delete your information from Google's systems.
3.	(2) The guarantee of confidentiality as referred to in paragraph (1) shall be carried out through the stipulation of security classification, access restriction, and other security control.	Google takes the confidentiality of your data seriously. Refer to our Google Cloud Privacy Commitments for additional info around how we work to safeguard your data. Refer to Row 2 for information on Google's security practices.
4.	(3) The guarantee of integrity as referred to in paragraph (1) shall be carried out through the detection of modification.	Refer to Row 2 for information on Google's security practices. Integrity use of your 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.
5.	(4) The guarantee of availability as referred to in paragraph (1) shall be carried out through the provision of backup and recovery.	Refer to Row 2 for information on Google's security practices. The SLAs contain Google's commitments regarding availability of the Services. They are available on the Google Cloud Platform Service Level Agreements page. 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. Google will not make updates that materially reduce the functionality, performance, availability or security of the Services.More information is available on our Incidents & the Google Cloud dashboard page.
6.	(5) The guarantee of authenticity as referred to in paragraph (1) shall be carried out through the provision of verification and validation mechanism.	Refer to Row 2 for more information on Google's security practices.

REGULATION OF THE PRESIDENT OF THE REPUBLIC OF INDONESIA NUMBER 95 OF 2018

Google Cloud Mapping

		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 on the Google Cloud Encryption at rest page. • **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 on the Google Cloud Encryption in transit page. Additionally, Google allows you to easily encrypt your data in the cloud using software-backed encryption keys, FIPS 140-2 Level 3 validated HSMs, customer-provided keys or an External Key Manager to help customers on their journey to ensure authentication mechanisms are in place. . You can use customer-managed encryption keys (CMEK) to control the encryption of data across Google Cloud products while benefiting from additional security features such as Google Cloud IAM and audit logs. Google maintains policies and procedures that enforce data access permissions. Two factor authentication is required for all employee access to all company and customer resources. Google provides (under NDA) customers with a SOC 2 report that includes testing of Google's access controls.
7.	(6) The guarantee of non repudiation as referred to in paragraph (1) shall be carried out through the application of digital signature and guarantee of trusted third party through the use of digital certificate.	This is a customer consideration.
8.	**Article 41**	
9.	(1) Each Central Agency and Regional Government must apply SPBE Security.	This is a customer consideration.
10.	(2) In applying SPBE Security and setting problems in SPBE Security, the head of the Central Agency and head of region may carry out consultation and/or coordination with the head of institution who organizes government tasks in the field of cyber security.	This is a customer consideration. Refer to Row 2 for more information on Google's security practices.
11.	(3) Application of SPBE Security must meet the technical standards and procedures of SPBE Security.	This is a customer consideration. Google will comply with all laws and regulations applicable to it in the provision of the Services.

REGULATION OF THE PRESIDENT OF THE REPUBLIC OF INDONESIA NUMBER 95 OF 2018

Google Cloud Mapping

12.	(4) Further provisions on technical standards and procedures of SPBE Security shall be stipulated by a Regulation of the Institution that organizes government tasks in the field of cyber security.	This is a customer consideration.
13.	**Article 46**	
14.	(1) SPBE management shall include: a. risk management; b. information security management; c. data management; d. information and communication technology asset management; e. human resource management; f. knowledge management; g. change management; and h. SPBE Service management.	This is a customer consideration.
15.	(2) The Central Agency and Regional Government shall implement the SPBE Management as referred to in paragraph (1).	This is a customer consideration.
16.	(3) The Implementation of SPBE Management as referred to in paragraph (2) shall be based on the Indonesian National Standard.	This is a customer consideration. Google will comply with all laws and regulations applicable to it in the provision of the Services.
17.	(4) In the event that the Indonesian National Standard as referred to in paragraph (3) is not yet available, the implementation of SPBE Management may be based on the international standard.	This is a customer consideration. Google will comply with all laws and regulations applicable to it in the provision of the Services.
18.	**Article 47**	
19.	(1) The risk management as referred to in Article 46 paragraph (1) sub-paragraph (a) shall be aimed to guarantee the sustainability of SPBE by minimizing the impacts of risk in SPBE.	This is a customer consideration. Information about Google's approach to risk management is available in Google's certifications and audit reports Google recognizes that regulated 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)

		• ISO/IEC 27701:2019 (PII) • PCI DSS • SOC 1 • SOC 2 • SOC 3 You can review Google's current certifications and audit reports at any time. Google provides comprehensive external documentation and whitepapers detailing our security infrastructure and operational model. Google also maintains an internal ISMS as a risk management framework and evidence of its effectiveness is provided via ISO/IEC 27001 certification. • Google's ISO certifications are available here. • Google's SOC reports and PCI Attestation of Compliance (AOC) are available via your Google Cloud account representative. Customers may provide these materials to their regulatory agencies.
20.	(2) Risk management shall be carried out through a series of identification, analysis, control, monitoring and evaluation processes to the risk in SPBE.	Refer to Row 19 for more information.
21.	(3) The risk management as referred to in paragraph (2) shall be implemented based on guidelines on risk management of SPBE.	This is a customer consideration. Information about Google's approach to risk management is available in Google's certifications and audit reports. Refer to Row 19 for more information. You can review Google's current certifications and audit reports at any time.
22.	(4) In the implementation of risk management, the head of the Central Agency and head of region shall coordinate and may carry out consultation with the minister who organizes government affairs in the field of state apparatus.	This is a customer consideration.
23.	(5) Further provisions on guidelines on risk management of SPBE shall be stipulated by a Regulation of the Minister who organizes government affairs in the field of state apparatus.	This is a customer consideration.
24.	**Article 48**	
25.	(1) The information security management as referred to in Article 46 paragraph (1) sub-paragraph b shall be aimed to guarantee the sustainability of SPBE by minimizing the impacts of risk in information security.	Refer to Row 2 for more information on information security and management.
26.	(2) Information security management shall be carried out through a series of processes including determination of scope, assignment of person in charge,	Refer to Row 2 for more information.

	planning, operational support, performance evaluation, and continuous improvement in information security in SPBE.	Monitoring 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. • Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP. • 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).
27.	(3) The information security management as referred to in paragraph (2) shall be implemented based on guidelines on information security management of SPBE.	This is a customer consideration. Refer to Row 25 for more information.
28.	(4) In the implementation of information security management, the head of the Central Agency and head of region shall coordinate and may carry out consultation with the head of institution who organizes government tasks in the field of cyber security.	This is a customer consideration.
29.	(5) Further provisions on guidelines on information security management of SPBE shall be stipulated by a Regulation of the Institution that organizes government tasks in the field of cyber security.	This is a customer consideration.
30.	**Article 49**	
31.	(1) The data management as referred to in Article 46 paragraph (1) sub-paragraph c shall be aimed to guarantee the realization of accurate, up-to-date, integrated and accessible data as the basis for planning, implementation, evaluation and controlling the national development.	Refer to Row 2 for information on Google's security practices. Google will comply with all national data protection regulations applicable to it in the provision of the Services. In addition, Google makes commitments to protect your data, including regarding security, access and transfer in the Cloud Data Processing Addendum. **Use of your information** You can provide Google instructions about your data and Google will comply with those instructions.

		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. **Privacy and NonPublic Personal Information** The Cloud Data Processing Addendum address the roles and responsibilities of the parties for your data. In particular, Google will: • comply with privacy laws and regulations applicable to it in the provision of the Services. • 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. • enable you to delete your information and comply with your instruction to delete your information from Google's systems. 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.
32.	(2) Data management shall be carried out through a series of management processes of data architecture, master data, reference data, database, and data quality.	Refer to Row 31 for more information.
33.	(3) The data management as referred to in paragraph (2) shall be implemented based on guidelines on data management of SPBE.	This is a customer consideration. Refer to Row 31 for more information.

REGULATION OF THE PRESIDENT OF THE REPUBLIC OF INDONESIA NUMBER 95 OF 2018

Google Cloud Mapping

34.	(4) In the implementation of data management, the head of the Central Agency and head of region shall coordinate and may carry out consultation with the minister who organizes government affairs in the field of national development planning.	This is a customer consideration.
35.	(5) Further provisions on guidelines on data management of SPBE shall be stipulated by a Regulation of the Minister who organizes government affairs in the field of national development planning.	This is a customer consideration.
36.	**Article 50**	
37.	(1) The Information and Communication Technology asset management as referred to in Article 46 paragraph (1) sub-paragraph d shall be aimed to guarantee the availability and optimization of utilization of information and communication technology asset in SPBE.	This is a customer consideration. Availability Google's global infrastructure delivers the highest levels of performance and availability in a secure, sustainable way. Refer to our Google Cloud Infrastructure page for more information about our network and facilities. In addition, Google maintains policies and procedures to ensure consideration of availability throughout the entire Customer engagement. Google provides customers with uptime availability metrics and industry standard audit reports and certifications. Google maintains a dashboard for service availability information and service issues: https://status.cloud.google.com/
38.	(2) Information and Communication Technology asset management shall be carried out through a series of planning, procurement, management and removal processes of hardware and software used in SPBE.	Deletion On termination of the contractual relationship, Google will comply with your instruction to delete customer data from Google systems. Google has strict policies and procedures to govern the management of the equipment lifecycle within its production data centers. Any disk that did, at any point in its lifecycle, contain customer data is subject to a series of data destruction processes before leaving Google's premises, and would need to be authorized by the appropriate operations manager before release. For more information, please see: data deletion on GCP, media sanitization process and the decommissioned disks and disk erase policy in the Cloud Data Processing Addendum. Refer to Row 37 for more information.
39.	(3) Management of information and communication technology assets as referred to in paragraph (2) is implemented based on technology asset management guidelines SPBE information and communication.	This is a customer consideration. Customers may leverage Cloud Asset Inventory to view, monitor, and analyze all of their GCP assets.

REGULATION OF THE PRESIDENT OF THE REPUBLIC OF INDONESIA NUMBER 95 OF 2018

Google Cloud Mapping

		For its part, Google maintains assets inventories and assigns ownership for managing its critical resources. Google also tags physical hardware. Components are inventoried for easy identification and tracking within Google facilities. Other hardware characteristics, such as MAC are used for identification.
40.	(4) In implementing technology asset management information and communication, heads of the Central Agency and regional heads coordinate and consult with the minister that carry out government affairs in the field communication and informatics.	This is a customer consideration.
41.	(5) Further provisions regarding guidelines information and communication technology asset management SPBE governed by the Regulation of the Minister of the carry out government affairs in the field communication and informatics.	This is a customer consideration.
42.	**Article 55**	
43.	(2) Information and Communication Technology Audit includes examination of technical subject matter at: a. the application of governance and technology management information and communication b. information technology functionality and communication; c. performance technologies of information and communication that generated; and d. aspects of information and communication technology.	This is a customer consideration. Refer to Row 19 for information on the audit reports that Google provides. To ensure that they remain an effective tool, if a key system or control for a Service is not covered by Google's certifications or audit reports for that service, regulated entities can request an expansion of the scope. You can review Google's current certifications and audit reports at any time.
44.	(5) Provisions more about the policy general conducting Information Technology Audit and Communication regulated by the Regulation of the Minister of the carry out government affairs in the field communication and informatics.	This is a customer consideration. Refer to Row 43 for more information.
45.	**Article 56**	
46.	(2) National SPBE Infrastructure Audit as referred to in paragraph (1) letter a is implemented 1 (one) time in 1 (one) year by the head of the institution non ministerial government ones carry out government duties in the field assessment and application of technology.	This is a customer consideration. Refer to Row 19 for information on the audit reports that Google provides. The customer is best placed to decide what audit frequency and scope is right for their organization. Our contract does not limit customers to a fixed number of audits or a pre-defined scope.
47.	(3) The audit of SPBE Infrastructure of Central Agency and Regional Government as referred to in paragraph (1) sub-paragraph b shall be implemented not less than 1 (one) time in 2 (two) years by the Central Agency and Regional Government.	This is a customer consideration. Refer to Row 19 for information on the audit reports that Google provides.

		The customer is best placed to decide what audit frequency and scope is right for their organization. Our contract does not limit customers to a fixed number of audits or a pre-defined scope.
48.	(4) The audit of National SPBE Infrastructure as referred to in paragraph (2) and Audit of SPBE Infrastructure of Central Agency and Regional Government as referred to in paragraph (3) shall be implemented based on standards and procedures for the implementation of audit of SPBE Infrastructure.	This is a customer consideration. Refer to Row 19 for information on the system security standards that Google complies with.
49.	(5) In implementing the audit of SPBE Infrastructure of Central Agency and Regional Government as referred to in paragraph (4), the Central Agency and Regional Government shall coordinate with the minister who organizes government affairs in the field of communication and informatics related to the monitoring, evaluation, and reporting of audit of SPBE Infrastructure of Central Agency and Regional Government.	This is a customer consideration.
50.	(6) Further provisions on standards and procedures for the implementation of audit of SPBE Infrastructure shall be stipulated by a Regulation of Non-Ministerial Government Institution that organizes government tasks in the field of technology assessment and application.	This is a customer consideration. Refer to Row 19 for information on the audit reports that Google provides.
51.	**Article 58**	
52.	(2) The audit of SPBE Security as referred to in paragraph (1) shall be implemented based on standards and procedures for the implementation of audit of SPBE Security.	This is a customer consideration. Refer to Row 19 for information on the system security standards that Google complies with.
53.	(3) The audit of security of National SPBE Infrastructure as referred to in paragraph (1) sub-paragraph a and audit of security of General Application as referred to in paragraph (1) sub-paragraph c shall be implemented 1 (one) time in 1 (one) year by the head of institution who organizes government tasks in the field of cyber security.	This is a customer consideration. Refer to Row 19 for information on the audit reports that Google provides. The customer is best placed to decide what audit frequency and scope is right for their organization. Our contract does not limit customers to a fixed number of audits or a pre-defined scope.
54.	(4) The audit of security of SPBE Infrastructure of Central Agency and Regional Government as referred to in paragraph (1) sub-paragraph b and audit of security of Special Application as referred to in paragraph (1) sub-paragraph d shall be carried out not less than 1 (one) time in 2 (two) years by the Central Agency and Regional Government.	This is a customer consideration. Refer to Row 19 for information on the audit reports that Google provides. The customer is best placed to decide what audit frequency and scope is right for their organization. Our contract does not limit customers to a fixed number of audits or a pre-defined scope.
55.	(5) In implementing the audit of security of SPBE Infrastructure of Central Agency	This is a customer consideration.

	and Regional Government and audit of security of Special Application as referred to in paragraph (4), the Central Agency and Regional Government shall coordinate with the minister who organizes government affairs in the field of communication and informatics related to monitoring, evaluation, and reporting of audit of security of SPBE Infrastructure of Central Agency and Regional Government and audit of security of Special Application.	
56.	(6) Further provisions on standards and procedures for the implementation of audit of SPBE Security shall be stipulated by a Regulation of Institution that organizes government tasks in the field of cyber security.	This is a customer consideration. Refer to Row 19 for information on the system security standards that Google complies with.