REPUBLIC OF THE PHILIPPINES

DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY

DEPARTMENT CIRCULAR NO. 010 JUN 02 2020
Series of 2020

RE : AMENDMENTS TO DEPARTMENT CIRCULAR NO. 2017 – 002, RE: PRESCRIBING THE PHILIPPINE GOVERNMENT'S CLOUD FIRST POLICY.

WHEREAS, the Department of Information and Communications Technology (DICT) is the primary policy, planning, coordinating, implementing, and administrative entity of the Executive Branch of the government that will plan, develop, and promote the national Information and Communications Technology (ICT) development agenda;[1]

WHEREAS, it is the declared policy of the State to promote the development and widespread use of emerging ICT, and to foster and accelerate the convergence of ICT and ICT-enabled facilities;[2]

WHEREAS, the DICT is authorized to formulate, recommend, and implement national policies, plans, programs and guidelines that will promote the development and use of ICT with due consideration to the advantages of convergence and emerging technologies;[3]

WHEREAS, Department Circular (DC) No. 2017-002, re: *Prescribing the Philippine Government's Cloud First Policy,* declared it the policy of the government to adopt a "cloud first" approach and for government departments and agencies to consider cloud computing solutions as a primary part of their infostructure planning and procurement;[4]

WHEREAS, the use of cloud computing offers the key advantages of giving access to the global system of solutions and services, and up-to-date digital innovations and services, in order to improve the citizen's experience with government;

WHEREAS, as a matter of global industry standards, cloud service providers maintain robust and up-to-date authentication systems and state-of-the-art technology to effectively address the continuing cybersecurity concerns of their end-users, and provide appropriate safeguards against the breach in the confidentiality, integrity, or availability of the services, applications, or data stored in the cloud;

WHEREAS, countries across the world, including Singapore, Kingdom of Saudi Arabia, United States, Canada, United Kingdom, Chile, Australia, among other jurisdictions, have adopted cloud-first and cloud-migration policies that have enabled their government's use of cloud services and cloud computing technologies for the effective, timely, cost-efficient, secure, and up-to-date development, deployment, and maintenance of integrated and inter-operable government digital systems and online services, for the faster, more efficient, and economical rendition of quality public service through the use of ICT;

[1] §5, Republic Act (RA) No. 10844.

[2] §2, RA 10844.

[3] §6, RA 10844.

[4] §5.1, Department Circular (DC) No. 2017-002.

WHEREAS, the broad range of data owned and possessed by the Philippine government necessitates the use of appropriate data classification schemes that consider the different levels of data sensitivity, and the impact of unauthorized disclosure, use, alteration, and destruction of data, for purposes of ensuring that the security controls and protection chosen by government agencies and instrumentalities in their cloud deployment models are commensurate to the associated data risks and vulnerabilities, with the end goal of maintaining secure data management systems that address relevant national security, confidentiality, and data privacy concerns;

WHEREAS, while flexibility, security, and cost-efficiency afforded by quality cloud computing services is favored, the Philippine government does not relinquish any power or control over its data by virtue of its adoption of the technology;

WHEREAS, Office of the President (OP) Memorandum Circular (MC) No. 78 s. 1964, as amended by OP MC 196 s. 1968, provides for rules governing security of classified matter in government offices;

WHEREAS, Executive Order No. 2 s. 2016, provided guidelines to operationalize in the Executive Branch the people's constitutional right to information, and the state policies for full public disclosure and transparency in the public service;

WHEREAS, in accordance with §9, Chapter 2, Book VII of the 1987 Revised Administrative Code, the Department has, since the issuance of DC 2017-002 continued with its agency rulemaking processes with due notice and public consultations, and duly considered the views submitted by interested parties and stakeholders from the public and private sectors, in an effort to address issues arising from policy implementation and its potential improvement in pursuit of public interest.

NOW, THEREFORE, in view of the foregoing, in the exigencies of the service, and pursuant to the provisions of existing laws, rules, and regulations, the following directives are hereby issued:

Section 1. Amendments to DC 2017-002.—The following amendments to the provisions of DC 2017-002, re: *Prescribing the Philippine Government's Cloud First Policy,* are hereby instituted:

> **Section 1.1.** The provisions of **§3.1, et. seq., of DC 2017-002** on the coverage of the Cloud First Policy are hereby amended to read as follows:
>
> > *"3.1. This Circular shall cover all executive departments, bureaus, offices, agencies, and instrumentalities of the National Government, including Government Owned and/or Controlled Corporations (GOCCs) and their subsidiaries, State Universities and Colleges (SUCs), and Local Government Units (LGUs). The implementation of this Circular shall likewise cover cloud service providers, intermediaries, and other private entities with transactions, contracts, or data related to, in connection with, or arising from the rendition of cloud computing services for the Philippine government.*
> >
> > *3.2. The Philippine Congress, the Judiciary, the Independent Constitutional Commissions, and the Office of the Ombudsman, are hereby encouraged to adopt the Cloud First Policy counterparts for their respective institutions in accordance*

with the provisions of the Philippine Constitution, existing laws, circulars, rules, and regulations. Whenever necessary, the DICT may be requested to provide technical expertise and assistance in the development thereof."

Section 1.2. The provisions of **§5.2, et seq., of DC 2017-002** on the Philippine government's general adoption of cloud computing for the storage, use, and processing of its data are hereby amended to read as follows:

"5.2. In the storage, use, and processing of data, all government agencies and instrumentalities of the Republic of the Philippines shall adopt cloud computing as the preferred ICT deployment strategy, method, or technology for administrative use, or for the delivery of government services. By way of exception, ICT deployment strategies, methods, or technologies other than cloud computing may be utilized provided that the agency or instrumentality presents adequate, reasonable, and well-reasoned justifications to conclude that:

a) No cloud computing deployment strategy, method, or technology can meet its requirements; or

b) Its proposed use of the alternative ICT deployment strategy, method, or technology is superior to cloud computing based on the following characteristics:

i. Security,
ii. Features,
iii. Cost-effectiveness, and
iv. Deployability, defined in terms of:
a. ease of deployment
b. frequency of deployment, and
c. overall risk of deployment.

5.3. Whenever deemed necessary to ensure the resilience of data, systems, or platforms through redundancy, the government agency or instrumentality may utilize additional ICT deployment strategies, methods, or technologies to back-up or supplement its previously deployed ICT strategy, method, or technology.

5.4. Nothing in this Circular shall be construed to authorize the government agency or instrumentality's use of ICT deployment strategies, methods, or technologies that are not compliant with current applicable local and international standards and best practices on design, infrastructure, security, and operations. All government agencies and instrumentalities shall, in each of their respective project proposals and terms of reference for ICT deployment, indicate the standards and best practices applicable thereto, and their adherence or compliance therewith. For this purpose, government agencies or instrumentalities may request the DICT for technical assistance.

5.5. For capacity building and development of the essential skills relating to compliance with local and international standards and best practices for ICT design, infrastructure, security, and operations, all government agencies and instrumentalities shall provide adequate human resource development for select *personnel to undergo relevant and appropriate trainings, seminars, and certification courses and programs at the DICT or its partner institutions."*

Section 1.3. The provisions of **§9.2, et seq., of DC 2017-002** on data classification are hereby amended to read as follows:

> *"9.2. In view of the broad range of data owned or possessed by the Philippine Government, all heads of government agencies or instrumentalities shall determine, based on its institutionalized protocols and guidelines how each of their information or data shall be classified pursuant to the Data Classification Table (Attached as* **Annex "B"** *of this Circular for reference and guidance) for purposes of cloud computing, with due consideration of all factors relevant to the data to be stored and/or processed, such as but not limited to, the data's level of sensitivity; the risk of breach in the confidentiality, integrity, or availability of the data, and the potential impact thereof to the agency or instrumentality concerned, and the Philippine government as a whole; the prevailing ICT industry standards and best practices on the handling and security of the data; and other existing laws, policies, rules, and regulations applicable to the data.*
>
> *9.3. In determining its Data Classification Model vis-à-vis the appropriate baseline controls and security protocols for safeguarding data, the government agency or instrumentality shall be guided by the following enumeration, in descending order:*
>
> *a.* ***Highly Sensitive Government Data.****—Highly Sensitive Government Data shall include official matter classified as 'Top Secret,'*[5] *"Secret,"* [6] *and other similar data. Highly Sensitive Government Data may be stored or processed in the cloud only when necessary, in which case the government agency or instrumentality shall utilize a secure private cloud hosted in on-premise infrastructure that is within the Philippine territory or in other territories over which the Philippines exercises sovereignty or jurisdiction, such as but not limited to Philippine embassies and consulates. Highly Sensitive Government Data in the cloud shall at all times be subject to specific encryption requirements consistent with the standard of care and protection higher than that prescribed for sensitive and above-sensitive data.*
>
> *b.* ***Above-Sensitive Government Data.****—Above-Sensitive Government Data shall include official matter classified as "Confidential,"*[7] *and other similar data. Above-Sensitive Government Data may be stored and processed in the cloud, in which case the government agency or instrumentality shall utilize accredited public cloud hosted in in-country infrastructure, or the Philippine GovCloud. Above-Sensitive Government Data shall at all times be*

[5] *See §II, Office of the President (OP) Memorandum Circular (MC) No. 78 s. 1964, entitled "Security of Classified Matter in Government Departments and Instrumentalities," as amended by OP MC 196 s. 1968, Executive Order No. 608 s. 2007, §7(c) of Republic Act No.6713, and other related laws and executive issuances.*

[6] § III, *id.*

[7] §IV, *id.*

subject to specific encryption requirements consistent with the standard of care and protection higher than that prescribed for sensitive data. The government agency or instrumentality may, in its sound discretion, allow above-sensitive data that is stored or processed in in-country infrastructure to be likewise stored in off-shore infrastructure to ensure resiliency through redundancy.

c. ***Sensitive Government Data.***—*Sensitive Government Data shall include official matter classified as "Restricted,"*[8] *and other similar data. Sensitive Government Data may be stored in the cloud, in which case the government agency or instrumentality shall utilize accredited public cloud, whether in-country or off-shore, or the Philippine GovCloud. Sensitive Government Data shall at all times be subject to encryption requirements consistent with the degree of protection prescribed under existing laws, policies, rules, and regulations.*

d. ***Non-Sensitive Government Data.***—*Non-Sensitive Government Data shall include open and available data, publicly accessible data, un-classified data, and other similar data. Government agencies or instrumentalities may store or process their non-sensitive data using accredited CSPs, whether in-country or off-shore, or in the Philippine GovCloud.*

For collections of data with different sensitivity levels that need to be singularly classified in order to determine the appropriate cloud deployment model, the classification shall be based on the highest sensitivity level of any individual data within that collection.

9.4. The government agency or instrumentality shall select the appropriate cloud deployment model, whether private, hybrid, or public, located offshore or in-country, based on its classification of the data to be stored or processed therein, with due consideration of the following factors: (a) the agency or instrumentality's specific needs, (b) the cost-effectiveness of the deployment model, (c) the existence of appropriate controls, security protocols, and redundancy protocols. The provisions of Section 10, 11, and 12 of this Circular on Security, Security Framework, Data Sovereignty, and Data Residency shall likewise be strictly observed.

Section 1.4. The provisions of **§10.1** of DC 2017-002 on **Security** are hereby amended to read as follows:

"10.1. With the enhancement of overall data security being one of the objectives for migrating government workloads and data onto the cloud, whether public, hybrid, or private, located in-country or off-shore, or onto the Philippine GovCloud, all government agencies and instrumentalities shall ensure that the risks and

[8] *See §V, Office of the President (OP) Memorandum Circular (MC) No. 78 s. 1964, entitled "Security of Classified Matter in Government Departments and Instrumentalities," as amended by OP MC 196 s. 1968, Executive Order No. 608 s. 2007, §7(c) of Republic Act No.6713, and other related laws and executive issuances.*

vulnerabilities associated with the data stored or processed using their chosen cloud deployment model are adequately and effectively addressed through appropriate controls and security protocols.

Accredited CSPs in GovCloud shall be certified appropriately, based on their continued compliance with current local and international security standards for their industry, and all relevant Philippine laws."

Section 1.5. §12 of DC 2017-002 on **Data Sovereignty** and **Data Residency** is hereby amended to read as follows:

"SECTION 12. DATA SOVEREIGNTY AND DATA RESIDENCY

12.1. Data Sovereignty

All data created, collected, organized, modified, retrieved, used, consolidated, sourced from, or owned by the Philippine government, including all its agencies and instrumentalities, or by any national of the Philippines or any entity that has links to the Philippines, which are in the cloud, regardless of location, shall be governed by Philippine laws, policies, rules, and regulations.

Except as otherwise permitted under Philippine law, no such data shall be subject to foreign laws, or be accessible to other countries, regardless of the cloud deployment model used, the nationality of the CSP, or the data's place of storage, processing, or transmission. No rights appurtenant to such data shall be deemed transferred or assigned by virtue of the storage, processing, or transmission thereof by the CSP.

CSPs and other entities engaged in the storage, processing, or transmission of such data shall comply with all applicable Philippine laws, policies, rules, regulations, and issuances relating to data sovereignty, security, and confidentiality, inclusive of R.A. 10844, R.A. 10173, R.A. 10175, their implementing rules and regulations, and the provisions of this Circular.

12.2. Data Residency

As a general rule, no residency restrictions shall be placed on government data stored or processed in the cloud, provided that appropriate controls and security measures are present. By way of exception, the storage or processing of sensitive, above-sensitive, and highly-sensitive government data in the cloud shall be subject to the following:

a. *For* **Sensitive Government Data** *stored or processed in the cloud, the data residency shall be restricted to:*
   i. The Philippine territory,
   ii. Other territories over which the Philippines exercises sovereignty or jurisdiction, or
   iii. Other countries or states with which the Philippines has enforceable extradition treaties for the turn-over of persons accused or convicted

of violating Philippine laws, provided that such other countries or states shall have:

1. *Similar or higher standards of protection for Philippine government data as Philippine laws and issuances; or*
2. *Existing agreements with the Philippine government for the provision of similar or higher protection to Philippine government data as Philippine laws and issuances.*

*b. For **Above-Sensitive Government Data** stored or processed in the cloud, the data residency shall as far as practicable be limited to infrastructure within the Philippine territory or other territories over which the Philippines exercises sovereignty or jurisdiction. When necessary to ensure resiliency through redundancy, above sensitive data already stored or processed in in-country infrastructure may likewise be stored in off-shore infrastructure, subject to the requirements of the Section 12.2.(a)(iii) of this Circular.*

*c. For **Highly Sensitive Government Data** stored or processed in the cloud, the data residency shall be restricted to on-premise infrastructure that is within the Philippine territory or other territories over which the Philippines exercises sovereignty or jurisdiction such as but not limited to Philippine embassies and consulates.*

Nothing in this Circular shall be construed as a waiver on the part of the Philippine government of its power, authority, or discretion to determine where particular classes of data shall be stored or processed."

Section 1.6. Subsection 14.1 of §14 DC 2017-002 on **Data Ownership** is hereby amended to read as follows:

"14.1. Data Ownership

The Philippine government, its agencies, and instrumentalities shall retain full control and ownership over their data. CSPs shall at all times (a) provide identity and access controls to restrict access to infrastructure and data in favor of the Philippine government, its agencies, and instrumentalities, as end users; and (b) make options available to government agencies and instrumentalities on the storage, management, security, and protection of their data. CSPs shall not require long-term contracts or exclusivity.

There shall be no transfer, storage, or processing of government data in cloud infrastructure unless made in accordance with the provisions of this Circular and other relevant laws, policies, rules, regulations, and issuances.

Regardless of the management, ownership, operation, or location of the CSP, and to the exclusion of foreign governments, the Philippine government shall have the sole authority to determine the management, use, processing, storage, security, and accessibility of its data, with sole control over the encryption keys thereto, subject to *the requirements of the Philippine Constitution and Philippine laws, rules and regulations, and other issuances."*

Section 2. Automatic Incorporation.—Any contractual stipulation to the contrary notwithstanding, the provisions of DC 2017-002, as amended, shall be deemed written into or incorporated in all contracts, agreements, and documents signed and entered into by the head of agency, or his/her duly authorized representative, in relation to government and private data in the possession of the government agency or instrumentality.

Section 3. Reservation Clause.—Nothing in this Circular shall be construed to limit, decrease, or restrain the Department's authority and mandate under RA 10844, the Revised Administrative Code, and other existing laws, rules and regulations, and issuances.

Section 4. Separability Clause.—If any section, subsection or part of this Circular is held unconstitutional, invalid, illegal, or unenforceable, the constitutionality, validity, legality, and enforceability of the remaining sections, subsections or parts of this Circular shall not in any way be affected or impaired thereby, and shall remain valid and subsisting.

Section 5. Repealing Clause.—This Circular amends the relevant provisions of DC 2017-002. All other circulars, departmental issuances, or parts thereof, inconsistent with this Circular are hereby amended, modified, repealed or superseded, accordingly.

Section 6. Effectivity.—In view of the declared state of public health emergency and the imposition of the enhanced community quarantine affecting Luzon and other areas in the Philippines, this Circular shall take effect immediately upon its filing/publication in accordance with Section 4, Chapter 2, Book VII of the 1987 Revised Administrative Code.

Let copies of this Circular, together with DC 2017-002, as amended, be posted and published in the official DICT website and bulletin boards, as well as in a newspaper of general circulation, if available in light of the public health emergency.

GREGORIO B. HONASAN II
Secretary

Copy furnished:
All concerned.

Annex B

DATA CLASSIFICATION MODEL FOR CLOUD COMPUTING		
Public Sector Data Classification	**Suggested Baseline Cloud Deployment Model**	**Data Examples**
Non-sensitive data	Accredited public cloud, whether in-country or off-shore, or Philippine GovCloud.	Open data; publicly available data; unclassified data; data involving matters of public concern, which disclosure is allowed under Section 7 of the 1987 Philippine Constitution, and the orders, issuances, and laws operationalizing it; non-sensitive data as defined in Memorandum Circular (MC) No. 78 s. 1964, including informational websites, terminology systems, standards, practitioner registries, and similar data.
Sensitive data	Accredited public cloud, whether in-country or off-shore, or in the Philippine GovCloud, subject to encryption requirements consistent with the degree of protection prescribed under existing laws and executive issuances.	Business data, email, and CRM systems. Examples include financial records and medical records such as personally identifiable education records, personally identifiable financial information (PIFI), protected health information; official data classified as "Restricted" under MC 78 s. 1964, and the like, which may include: a. Departmental books of instruction and training and technical documents intended for official use only or not intended for release to the public; b. Routine information relating to the supply and procurement of military stores; c. Minor modifications and routine tests of equipment; and d. Certain compilations of data or items which individually may be unclassified but which in the aggregate warrant a classification.
Above–Sensitive Data	Accredited in-country public cloud, or the Philippine GovCloud. The government agency or instrumentality may, in its discretion, allow sensitive data stored and/or processed in in-country premises to be likewise stored in off-shore infrastructure in order to ensure resiliency through redundancy. Above-Sensitive data shall at all times be subject to specific encryption requirements consistent with the	Official data classified as "Confidential," under MC 78 s. 1964, and the like. It may include: a. Plans of Government projects such as land development, hydro electric schemes, road development, or development of areas; b. Routine Service reports, e.g., on operations and exercises, which contain information of value but not of vital interest to a foreign power; c. Routine Intelligence reports; d. Technical matter not of major importance but which has a distinct military value or requires protection otherwise, e.g., new weapons calculated to influence minor tactics or service tests of war equipment of a standard pattern; e. Certain personnel records and staff matters; f. Certain compilations of data or items which individually may be classified RESTRICTED, or which may be unclassified, but the aggregation of which enhances their security value; g. Matters, investigations and documents of a personal and disciplinary nature, the knowledge of which is desirable to safeguard for administrative reasons; and

DATA CLASSIFICATION MODEL FOR CLOUD COMPUTING		
Public Sector Data Classification	**Suggested Baseline Cloud Deployment Model**	**Data Examples**
	standard of care and protection higher than that prescribed for sensitive data.	h. Identification of personnel being investigated for misconduct, anomaly or fraud prior to the filing of appropriate charges or completion of the findings of boards created for such purpose.
Highly Sensitive Data	May be stored or processed in the cloud only if necessary, in which case, a secure private cloud hosted in on-premise infrastructure within the territory or in other territories over which the Philippines has jurisdiction, shall be utilized. Highly Sensitive data shall at all times be subject to specific encryption requirements consistent with the standard of care and protection higher than that prescribed for sensitive and above-sensitive data.	Official data falling classified as "Top Secret" and "Secret," under MC 78 s. 1964, and the like. It may include: a. Very important political documents dealing with such matters as negotiations for major alliances; b. Major governmental projects such as drastic proposals to adjust the nation's economy (before official publication); c. Matter relating to new and far reaching experimental, technical and scientific developments in methods of warfare or defense, e.g., vital matter relating to atomic warfare, defense against biological warfare, or matter affecting future operational strategy; e. Information which would indicate the capabilities or major successes of our intelligence services or which would imperil secret sources; f. Critical information about cryptography in so far as it relates to devices and equipment under development; g. Certain compilations of data or items which individually may be classified SECRET or lower, but which collectively should be put in a higher grade; h. High level directives dealing with important negotiations (as distinct from major negotiations which would be in the TOP SECRET category) with other countries; i. Proposals for new schemes of governmental or other controls, foreknowledge of which would seriously prejudice their operation; j. Matters relating to certain new methods of warfare or defense, including scientific and technical developments, not classified as TOP SECRET, e.g., new designs of Service aircraft, guided projectiles, tanks, radar and anti-submarine devices. A SECRET grading is justified if: (1) It materially influences a major aspect of military tactics; (2) It involves a novel principle applicable to existing important projects; (3) It is sufficiently revolutionary to result in a major advance in existing techniques or in the performance of existing secret weapons; (4) It is liable to compromise some other projects already so graded. k. Plans or details of schemes for the defense of areas other than vital strategic areas, including plans or particulars of operations connected with them. e. Vital military information, including photographs, maps, etc., relating to important defenses, establishments, and installations.

DATA CLASSIFICATION MODEL FOR CLOUD COMPUTING		
Public Sector Data Classification	**Suggested Baseline Cloud Deployment Model**	**Data Examples**
		f. Intelligence which is not in the TOP SECRET category but which would reveal a secret source, or the value of which depends upon concealing the fact that we possess it. g. Cryptographic devices and equipment unless specifically assigned to a lower classification. h. Certain compilations of data or items which individually may be classified CONFIDENTIAL or lower, but which collectively should be put in a higher grade. This generally includes political documents dealing with matters of international negotiations, technical matters of military value, major governmental projects such as proposals to adjust the nation's economy (before official publication) internal audit data, trade secrets, technical data supporting technology transfer agreements.