Republic of the Philippines
COMMISSION ON AUDIT
Commonwealth Avenue, Quezon City

CIRCULAR

No. : 2020-010
Date: DEC 0 2 2020

To : All Heads of Departments, Agencies, Bureaus, Offices and Instrumentalities of the National Government; Local Chief Executives; Managing Heads of Government-Owned and/or Controlled Corporations; Heads of Finance, Accounting and Treasury Units; Commission on Audit (COA) Assistant Commissioners, Directors, and Auditors; and All Others Concerned

Subject : Guidelines implementing COA Resolution No. 2020-034 relative to the Authority of COA Auditors to Access Information and Communications Systems, Electronic Data Messages and Source Documents of the Audited Entities Relevant to the Conduct of Audit

1.0 BACKGROUND

To effectively discharge the mandate of COA in safeguarding the government assets and to effectively perform audit procedure in this age of 4th Industrial Revolution, COA shall conduct information systems audit on government entities with computerized environment.

With the passage of the Republic Act No. 10173 otherwise known as the Data Privacy Act of 2012, there were instances when COA auditors were precluded by its auditees to access and perform the evaluation of the systems and their databases, especially those outsource-developed system due to data privacy issues.

Therefore, consistent with the mandate of COA to promote good governance through transparency and accountability, this Circular is hereby promulgated to implement COA Resolution No. 2020-034 dated December 2, 2020 and provide guidelines relative to the authority of COA Auditors to access information and communications systems and electronic documents of audited entities, with adherence to the general data privacy principles of the Data Privacy Act of 2012.

2.0 COVERAGE

This Circular shall apply to all audited entities that intend to use or which have been using information and communications systems in processing their functions and mandates regardless whether the system is developed in-house or outsourced.

3.0 DEFINITION OF TERMS

The following words and phrases are defined as follows:

3.1 **Audited Entity** refers to any department, bureau or office of the national government, or any of its branches and instrumentalities, or any political subdivision or local government units as well as any government-owned or controlled corporation, including its subsidiaries, or other self-governing board or commission of the government, which are subject to audit. These include other entities placed under the jurisdiction of COA by specific provisions of law or jurisprudence.

3.2 **Electronic Data Message** refers to information generated, sent, received or stored through electronic, optical or similar means.

3.3 **Electronic Document** refers to information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation is extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored, processed, retrieved or produced electronically.

3.4 **Data Protection Officer** refers to an individual/s who is accountable for ensuring compliance with applicable laws and regulations for the protection of data privacy and security.

3.5 **Information and Communications System** refers to a system intended for and capable of generating, sending, receiving, storing or otherwise processing electronic data messages or electronic documents and includes the computer system or other similar device by or in which data is recorded, transmitted or stored and any procedures related to the recording, transmission or storage of electronic data message or electronic document.

3.6 **In-house Developed System** refers to the system developed and implemented by the organization, the audited entity, using its own resources.

3.7 **Outsource-Developed System** is a system developed by a third-party provider.

3.8 **Source Document** refers to any document which serves as a basis for recording business transactions (invoice, official receipt, delivery receipt, disbursement voucher, etc.). This also includes technical documentation such as system

architecture, manuals, design decisions, and program source code, among others.

3.9 **Third-Party Provider** refers to a provider of –

(i) application systems and computer services necessary in the performance of government functions;

(ii) on-line services or network access, or the operator of facilities thereof, including entities offering the transmission, routing, or providing of connections for online communications, digital or otherwise, between or among points specified by a user, of electronic documents of the user's choosing; and

(iii) necessary technical means by which electronic documents of an originator may be stored and made accessible to a designated or undesignated recipient party.

4.0 GUIDELINES

4.1 COA auditors shall transmit a written request to the audited entities for a read/view, extract, and print access rights to the information and communications systems, electronic data messages and source documents with adherence to the general data privacy principles of transparency, legitimate purpose and proportionality. The request shall state the purpose and the specific data which are necessary to be accessed to meet its audit objectives.

4.2 Within five (5) working days after the receipt of the request, the audited entities shall provide COA auditors a unique user account to establish accountability in accessing information and communications system and electronic data. The audited entity may also share the electronic data electronically or provide the same through back up files created in the entity's environment and shared on a removable media with COA Auditors. The user account profile should have a read, view, print, and/or download capability.

4.3 Every contract/agreement shall be subject to COA audit. The auditability clause shall be provided in the contract pursuant to Section 39 of Presidential Decree No. 1445. The failure to provide the auditability clause in the contract with the third-party provider does not preclude COA from conducting the audit.

4.4 COA auditors shall treat all information gathered with appropriate level of confidentiality pursuant to existing laws, rules, and regulations, particularly those concerning data security and personal data protection. The Data Protection Officer of the audited entity should be informed before collection of pertinent personal data.

4.5 COA shall implement appropriate organizational, physical and technical security measures to protect the electronic data messages and documents obtained in carrying out their mandated functions.

4.6 COA shall capacitate its auditors to carry out their duties and responsibilities.

5.0 PENALTY CLAUSE

Failure or negligence of the officials or employees of audited entities to discharge their duties and responsibilities provided herein shall be a basis for appropriate administrative sanctions.

6.0 REPEALING CLAUSE

All circulars, memoranda, and other issuances or any parts thereof inconsistent with this Circular are hereby revoked, amended or modified accordingly.

7.0 SEPARABILITY CLAUSE

In the event that any of the provision of this Circular is declared invalid or unconstitutional, all the provisions not affected thereby shall remain valid and with legal effect.

8.0 EFFECTIVITY

This Circular shall take effect after fifteen (15) days from publication in newspaper of general circulation.

COMMISSION ON AUDIT
OFFICE OF THE COMMISSION SECRETARIAT

MICHAEL G. AGUINALDO
Chairperson

ROLAND C. PONDOC
Commissioner