Implementing Rules and Regulations of the E-Governance Act
(Republic Act No. 12254)

Pursuant to Section 38 of Republic Act (R.A.) No. 12254, otherwise known as "An Act Institutionalizing the Transition of the Government to E-Governance, Strengthening the ICT Academy, and Appropriating Funds Therefor" (Act), the following Implementing Rules and Regulations, hereinafter referred to as the IRR, are hereby promulgated:

RULE I
GENERAL PROVISIONS

SECTION 1. ***Title.*** — This IRR shall be known as the "2026 Implementing Rules and Regulations of the E-Governance Act".

SECTION 2. ***Declaration of Policy.*** — The State recognizes the vital role of information and communication in nation-building and the necessity of leveraging the power of information and communications technology (ICT) to drive national development and progress.

The State hereby adopts a policy to establish, foster, and sustain a digitally empowered and integrated government through the implementation of a regulated, secure, and robust information and communication system aimed at facilitating responsive and transparent online citizen-centered services, thereby optimizing the potential of open data for promoting economic growth while balancing the rights to freedom of information and data privacy of every Filipino.

SECTION 3. ***Purposes and Objectives.*** — The purposes and objectives of this IRR are to:

(a) define the roles and responsibilities of various agencies in the entire digital transformation process and provide effective leadership in developing and promoting electronic government services and processes;

(b) promote interoperability of government systems and processes through a consolidated process architecture, while allowing government agencies, offices, and instrumentalities to implement the proper controls and safeguards deemed appropriate on ICT and information assets;

(c) provide citizen-centered government information and services, and improve public trust and citizen participation in the government;

(d) enable access to government information and services, in accordance with the Constitution and relevant laws, while leveraging ICT and emerging technologies to enhance process efficiency, data security, and overall effectiveness;

(e) strengthen transparency and accountability efforts of the national and local governments;

(f) foster an informed and data-driven decision-making process for policymakers by utilizing data analytics results, among other pertinent factors;

(g) strengthen resilience against information technology disruptions, including, but not limited to, cybersecurity attacks, by incorporating best practices both from public and private sectors, locally and internationally;

(h) promote electronic transactions, particularly where mobility of citizens is restricted during disasters or pandemics;

(i) foster job creation, promote sustainability, and ensure up-to-date qualification and competency standards of ICT positions within the government;

(j) encourage sustainability and fortify manpower capabilities by continuously upskilling ICT professionals through the Academy; and

(k) reduce costs and burdens for businesses and other government entities.

SECTION 4. ***Coverage.*** — Subject to limitations under existing laws, this IRR shall apply to all executive, legislative, judicial, and constitutional offices, including local government units (LGUs), state universities and colleges (SUCs), government-owned or -controlled corporations (GOCCs), and other instrumentalities, whether located in the Philippines or abroad (collectively, "Covered Entities"), and their services that relate to business- and non-business-related transactions as defined in Republic Act (R.A.) No. 9485, as amended by R.A. No. 11032 or the "Ease of Doing Business and Efficient Government Service Delivery Act of 2018" (EODBA).

This IRR shall also apply to:

(a) back-end government operations within, between, and across agencies;

(b) government-to-government transactions, particularly those involving sharing and processing of data and information between and among government agencies for policy, planning, and decision-making purposes; and

(c) other similar government operations.

Nothing in this IRR shall be construed to derogate from the fiscal and administrative autonomy and independence of government entities under the Constitution and other pertinent laws.

SECTION 5. ***Definition of Terms.*** — The following definition of terms shall apply for purposes of this IRR:

(a) *Application Programming Interface (API)* refers to an intermediary that allows interaction between applications, programs, software components, systems, hardware, and micro-services of different individuals or organizations;

(b) *Blockchain* is a shared, immutable ledger that facilitates the process of recording transactions and tracking tangible or intangible assets in a business network, where virtually anything of value can be tracked and traded, reducing risk and cutting costs for all involved;

(c) *Change management* refers to the deliberate and structured approach to transitioning individuals, teams, and organizations from a current state to a desired future state of organizational success;

(d) *Chief Information Officer (CIO)* refers to a senior government official responsible for the development, planning, and implementation of the government entity's Information System

Strategic Plan (ISSP) or ICT plan, and management of the agency's ICT systems, platforms, and applications;

(e) *Chief Information Security Officer (CISO)* refers to the individual or entity responsible for carrying out functions and responsibilities relevant to cybersecurity in a government agency and who serves as the primary liaison of the agency to the Sectoral Computer Emergency Response Team and the National CERT. The CISO ensures that information resources and technologies are effectively protected; oversees the development, implementation, and enforcement of cybersecurity policies; and works alongside the CIO in procuring cybersecurity products and services, and managing disaster recovery and business continuity plans;

(f) *Computer Emergency Response Team (CERT)* or *Computer Security Incident Response Team (CSIRT)* refers to a specialized group responsible for preventing, detecting, analyzing, responding to, and assisting in recovering from cybersecurity incidents and threats that affect information and communication systems at the organizational, sectoral or national level, providing advisory services, vulnerability analysis, threat intelligence dissemination, and coordinated incident response across multiple stakeholders;

Agency CERT refers to a CERT of a government agency while Sectoral CERT refers to a CERT at the sectoral level and which coordinates with Agency CERTs.

National CERT (NCERT) refers to the CERT organized and managed by the DICT as the central coordinating body for all Agency and Sectoral CERTs;

(g) *Common Data Sets* refers to standardized collections of data elements that are uniformly defined, structured, and shared across multiple systems, organizations, or sectors to ensure interoperability, consistency, and data quality;

(h) *Critical Information Infrastructure (CII)* refers to the computer systems and/or networks, whether physical or virtual, and/or the computer programs, computer data, and/or traffic data that are vital to this country that the incapacity, destruction, or interference with such system and assets would have a debilitating impact on security, national or economic security, national health and safety, or any combination of those matters. Government sectors initially classified as CIIs are the following: transportation (land, sea, air), energy, water, health, emergency services, public finance, banking and finance, business process outsourcing, telecommunications, space, and media;

(i) *Digitalization* refers to the process of using digital technologies to enhance the operations of the government, and provide new revenue and value-producing opportunities;

(j) *Digital Transformation* refers to the process of optimizing, reconstructing, and integrating digital technology into all areas of government to maximize resource configuration, improve operational efficiency and innovation capability, and enhance value delivery of stakeholders;

(k) *E-Governance* refers to the use of ICT by the government to provide public services in a more friendly, convenient, affordable, efficient, and transparent manner. Further, it is the application of ICT for delivering government services through integration of various stand-alone systems, platforms, and applications between Government-to-Citizens (G2C), Government-to-Businesses (G2B), and Government-to-Government (G2G) services. It is often linked to back-office processes and interactions within the entire government framework;

(l) *E-Government* refers to the use of ICT by the government to enhance access to and delivery of government services for an efficient, responsive, ethical, accountable, and transparent government;

(m) *Emerging technologies* refers to rapidly developing technologies that are generally new, or current technologies finding new applications, whose development, practical applications, and impact are still uncertain. They are often perceived as disrupting the status quo and allowing for innovative solutions, such as in government service delivery. Emerging technologies shall include, but shall not be limited to, artificial intelligence, quantum computing, blockchain, autonomous systems, and similar innovations with similar characteristics;

(n) *Enterprise Architecture* refers to the structured framework that defines the principles, standards, and integrated design of government business processes, information flows, data assets, applications, and technology infrastructure. It provides a coherent blueprint that guides agencies in planning, implementing, and governing digital systems to ensure interoperability, security, efficiency, and alignment with national digital government objectives;

(o) *Government ICT workers* refers to government personnel performing ICT-related functions such as but not limited to systems and infrastructure development, implementation and maintenance, cybersecurity, data governance, data privacy, ICT Policy and Planning, and other ICT matters. Personnel of the EGov Unified Project Management Office (EGov UPMO), and government personnel designated as CIOs, CISOs, and working at CERTs/ CSIRTs shall also be considered as government ICT workers;

(p) *Government Internet Protocol Exchange (G/IPX)* refers to a secure, managed, and interoperable IP-based network infrastructure established to connect, integrate, and facilitate data exchange among government agencies;

(q) *ICT Assets* refer to any data, device, equipment, infrastructure, system, or component thereof, utilized to ensure or support the proper efficient operation and implementation of ICT-related programs and delivery of ICT services;

(r) *ICT Plan* refers to the sum of set of goals, measures, strategies, agenda, budget, and timeline for the implementation of ICT programs and projects and the use of ICT, including digital platforms, to deliver public services or otherwise perform government functions;

(s) *Information and Communications Technology (ICT)* refers to the totality of electronic means to access, create, collect, store, process, receive, transmit, present, regulate, and disseminate information;

(t) *Information Security* refers to the preservation of confidentiality, integrity and availability of information. This may also involve other properties, such as authenticity, accountability, non-repudiation, and reliability of information. For the purposes of this IRR, "cybersecurity" refers to the protection of ICT systems, networks, applications, and data in cyberspace, and is a subset of "information security" ;

(u) *Information Security Standards (ISS)* refer to generally accepted cybersecurity standards which aim to protect and secure the confidentiality, integrity, availability, authenticity, and non-repudiation of information;

(v) *Information Systems Strategic Plan (ISSP)* refers to the three (3)-year plan that serves as the government entity's roadmap for using ICT as a strategic resource to support the attainment

of its goals, mission, and vision. It is also a written expression that aims to coordinate national ICT plans, efforts, knowledge, information, resource-sharing, and database-building, and to link a government entity's ISSPs with national ICT goals;

(w) *Interoperability* refers to the ability of different operating and software systems, applications, and services to communicate and exchange data in an accurate, effective, and consistent manner with different platforms and agencies;

(x) *Major or material information security incident* refers to a single event or a series of unwanted or unexpected events whose nature and scope are determined to have or likely to have a significant impact on a government agency's network, such as causing the stoppage, disruption, or degradation of operations or compromising the integrity, confidentiality, or availability of the information transmitted within its network;

(y) *Master data* refers to the original, authoritative dataset validated and maintained by the government agency, also known as the "parent agency," that has the statutory mandate to collect, generate, and safeguard such data. Master data shall include, but is not limited to, civil registry records, national identification data, business registration data, taxpayer records, land records, and social security data;

(z) *Nonbusiness-related transaction* refers to all other government transactions not falling under Section 4(c) of R.A. No. 11032 or the "Ease of Doing Business and Efficient Government Service Delivery Act of 2018";

(aa) *Once-Only principle* refers to the approach ensuring that citizens and business entities only need to submit certain information and documents once when applying for government and public services. This entails government agencies re-using and sharing data with each other;

(bb) *Open Data* refers to data that can be freely used, reused and redistributed by anyone, subject to proper attribution and sharing;

(cc) *Personal data* refers to all types of information pertaining to an individual including personal information, sensitive personal information, and privileged information, as defined under R.A. No. 10173 or the Data Privacy Act (DPA) and its IRR;

(dd) *Personal information* refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual;

(ee) *Personal Information Controller (PIC)* refers to any natural or juridical person who controls the collection, holding, processing or use of personal data, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal data on his or her behalf. The term excludes:

(1) A person or organization who performs such functions as instructed by another person or organization; and

(2) An individual who collects, holds, processes or uses personal data in connection with the individual's personal, family or household affairs.

(ff) *Personal information processor* (PIP) refers to any natural or juridical person qualified to act as such under the DPA to whom a PIC may outsource the processing of personal data;

(gg) *Public Key Infrastructure (PKI)* refers to the framework of policies, technologies, and procedures used to create, manage, distribute, use, store, and revoke digital certificates and public-key encryption. PKI enables secure electronic transactions, authentication, confidentiality, integrity, and non-repudiation of data and communications across digital networks;

(hh) *Privacy-by-Default* refers to the principle according to which the PIC and PIP ensures that only data necessary for each specific purpose of processing is processed by default, without the intervention of the data subject;

(ii) *Privacy-by-Design* refers to an approach to the development and implementation of projects, programs, and processes that integrate into the design or structure safeguards that are necessary to protect and promote privacy into the design or structure of a processing activity or a data processing system;

(jj) *Privacy Engineering* refers to the integration of privacy concerns into engineering practices for systems and software engineering life cycle processes;

(kk) *Privacy Impact Assessment (PIA)* refers to the process undertaken and used to evaluate and manage impacts on privacy of a particular program, project, process, measure, system or technology product of a PIC or PIP. It takes into account the nature of the personal data to be protected, the personal data flow, the risks to privacy and cybersecurity posed by the processing, current data privacy best practices, the cost of cybersecurity implementation, and, where applicable, the size of the organization, its resources, and the complexity of its operations;

(ll) *Underserved areas* refer to areas that have unreliable and inadequate ICT services, as may be defined by the Department of Information and Communications Technology (DICT);

(mm) *Unserved areas* refer to areas that do not have data transmission industry participants and ICT services, as may be defined by the DICT;

(nn) *Vulnerability Assessment and Penetration Testing (VAPT)* refers to a comprehensive cybersecurity evaluation process used to identify, analyze, and address weaknesses or vulnerabilities in an organization's information systems, networks, applications, and infrastructure.

RULE II
IMPLEMENTING AGENCY

SECTION 6. ***Role of the Department of Information and Communications Technology (DICT).*** — The DICT shall be the lead implementing agency and administrator of the Act and this IRR, and shall exercise overall policy leadership, technical oversight, standards harmonization, and institutional coordination to ensure a coherent and interoperable national E-Governance ecosystem.

Subject to the Constitution and applicable laws, the DICT shall ensure that all national and local ICT projects in the Philippines are aligned and harmonized with the National ICT

Development Agenda and E-Government Master Plan (EGMP), and compliant with the measures, policies, and standards under the Act, this IRR, and relevant DICT issuances.

Accordingly, the DICT shall exercise the following powers and functions:

(a) Policy Formulation, Strategic Governance and Implementation.

(1) adopt national policies and processes that promote innovation, support start-ups, and facilitate the entry and adoption of technologies consistent with the objectives of the Act and this IRR;

(2) mandate and guide the adoption of policies and processes necessary for the implementation of the Act and this IRR, including the formulation of a strategic and phased whole-of-government E-Government roadmap with clearly defined milestones, roles, and responsibilities;

(3) pursuant to Section 10 of the Act, conduct a mandatory PIA, in accordance with relevant issuance of the National Privacy Commission (NPC), on the proposed systems for processing personal data included in the EGMP before its publication;

(4) ensure that all E-Government Programs comply with data privacy laws, and, when necessary, formally seek and incorporate guidance and assistance from the NPC on matters concerning the security and protection of personal data;

(5) on its own, or through other public or private entities, conduct research, surveys, and related studies to inform the formulation of E-Governance policies and plans, and the design of programs and projects, ensuring these are impartial, objective, and evidence-based; and

(6) prescribe the necessary measures, obligations, and standards to ensure the cybersecurity and resilience of CII that are essential for the operation and maintenance of critical government institutions.

(b) ICT Infrastructure, Systems, and Standards Oversight

(1) establish the EGov UPMO in accordance with Section 7 of the Act;

(2) oversee and guide the operation of ICT infrastructure, systems, and facilities in accordance with applicable laws and rules, including on cybersecurity;

(3) guide, monitor, and support government agencies in ensuring the quality, cybersecurity, reliability, and interoperability of ICT infrastructure and services in accordance with applicable standards and best practices, and provide necessary training, certification, and advisory support; and

(4) engage technical and standards organizations and consult industry experts on matters requiring specialized engineering, enterprise architecture, and cybersecurity other technical expertise.

(c) Inter-Agency Coordination and Public-Private Collaboration

(1) coordinate and collaborate with government agencies and the private sector, including through partnerships and joint ventures, to promote innovation and technology transfer and in furtherance of the objectives of the Act and this IRR; and

(2) receive grants and donations for the implementation of the Act subject to pertinent provisions of R.A. No. 3019 or the "Anti-Graft and Corrupt Practices Act", R.A. No. 6713 or the "Code of Conduct and Ethical Standards for Public Officials and Employees" and other relevant laws.

(d) ICT Human Resource Development and Competency Standards

(1) in coordination with the Civil Service Commission (CSC), mandate compliance by Covered Entities with minimum qualification and competency standards for all government ICT positions and require regular reporting on the status of compliance; and

(2) through the Academy, develop, in accordance with applicable civil service laws and rules, consistent with the compensation and position classification system of the government, the competency and qualification standards for all government ICT positions.

(e) Inclusive and Accessible E-Government

(1) ensure, as far as practicable, that E-Government Programs and platforms are inclusive and accessible to persons with disabilities.

(f) Monitoring, Compliance and Performance Assessment

(1) develop Performance Score Cards on the compliance of Covered Entities; and

(2) monitor implementation of E-Government programs and ISSPs to ensure alignment with the EGMP and its integrated framework.

In the implementation and enforcement of the foregoing, the DICT shall recognize the fiscal and administrative autonomy provided by the Constitution and other laws to independent government agencies, offices, and instrumentalities which shall independently undertake, supervise, and regulate their own ICT projects and shall only be required to coordinate and report to the DICT for alignment of policy objectives.

SECTION 7. ***Establishment of the E-Governance Unified Project Management Office (EGov UPMO).*** — Within one (1) year from the effectivity of the Act, EGov UPMO shall be established as a bureau-level organizational unit within the DICT. It shall be under the direct supervision and control of the Undersecretary for E-Government, or its equivalent. The EGov UPMO shall be responsible for addressing the portfolio, program, and project management needs of Covered Entities to ensure that all government ICT projects across the government are managed with operational efficiency and technical agility, consistent with international best practices and standards.

The DICT, in coordination with the CSC and the Department of Budget and Management (DBM), shall issue guidelines on the operation of the EGov UPMO within ninety (90) days from the effectivity of this IRR. The guidelines shall cover, among others, the organizational structure, staffing pattern, functions, operational procedures, performance management system,

and other administrative and technical matters necessary for the effective and efficient operation of the EGov UPMO.

SECTION 8. ***Functions of the EGov UPMO.*** — The EGov UPMO shall perform the following functions, among others:

(a) oversee, monitor, and provide technical guidance on the planning, execution, timeliness, performance and resource utilization of all government ICT projects and programs;

(b) ensure that the entire portfolio of E-Government Programs is aligned with the EGMP, the Philippine Government Interoperability Framework (PGIF), and other relevant national ICT plans, policies, and frameworks;

(c) prescribe and require compliance with internationally recognized best practices and standards in project, program, and portfolio management including but not limited to risk management, quality assurance, benefits realization, and change management; and

(d) coordinate with the Academy to ensure the systematic development and regular delivery of courses, including multimodal training and certification programs, and to implement capacity-building initiatives that enhance the skills, knowledge, and technical expertise of EGov UPMO and other DICT units responsible for the development and implementation of the Act.

SECTION 9. ***Qualifications of EGov UPMO Personnel.*** — Personnel appointed or assigned to the EGov UPMO shall be required to secure and maintain internationally recognized certifications and competency standards on Project Management, Program Management, Technology Management, IT Service Management, Enterprise Architecture, Information Security, Data Privacy, and Risk Management, Data Analytics, and ICT financial planning and budgeting, among others.

The Academy Act shall provide guidelines on the minimum qualifications for such certifications and competency standards for EGov UPMO personnel in accordance with Section 44 of this IRR.

SECTION 10. ***Transition of Existing DICT Offices to the EGov UPMO.*** — During the transition period, the DICT shall designate qualified existing personnel and an existing office with substantially similar or related functions to perform, on an interim basis, the functions of the EGov UPMO. Such qualified existing personnel may be designated based on competencies despite lacking the required certifications, provided they secure the necessary certifications within one (1) year from the date of assumption to the position. The DICT Secretary, may, for justifiable reasons and subject to existing laws, rules, and regulations, extend the period for compliance. This arrangement shall be without prejudice to any subsequent reorganization, reconstitution, or reappointment in accordance with the final guidelines to be issued. The DICT shall allocate to the EGov UPMO the funds necessary to carry out this purpose.

SECTION 11. ***Interagency Agreements for Implementation of E-Government Programs.*** — The DICT may enter into service agreements, memoranda of agreement, or other similar inter-agency arrangements with Covered Entities. Such arrangements may be undertaken through agency-to-agency procurement, inter-agency cooperation, or similar mechanisms, where the DICT is mandated by law or possesses the requisite technical capability, infrastructure, or institutional competence to deliver the required ICT systems, platforms, or services, consistent with the R.A. No. 12009 or the "New Government Procurement Act" (NGPA), and applicable issuances of the DBM and the Commission on Audit (COA).

SECTION 12. ***Collection of Fees.*** — In accordance with Section 33 of the Act, the DICT may collect reasonable fees from authorized sources for services directly related to the implementation, operation, and sustainability of the E-Government Programs, such as issuance of certifications or technical clearances expressly permitted by law, access to shared or common digital platforms, interoperability and data-exchange services, API access, hosting and cloud computing services, and cybersecurity services related to E-Government Programs and government CII. All fees collected shall accrue to the E-Government Interoperability Fund and shall be subject to existing budgeting, accounting, and auditing rules and regulations.

Fees, reimbursements, cost-sharing amounts, or fund transfers arising from services rendered or service agreements entered into under Section 11 shall be reasonable and sufficient to defray the minimum costs of providing the service and shall consider, among others, the available budget of the Covered Entity, operational and maintenance costs, cost recovery, cybersecurity requirements, system enhancements, cloud subscriptions, software licenses, and such other expenses necessary for the effective implementation of the E-Government Programs.

The DICT shall issue and publish guidelines for determining the fees, including any subsequent revisions thereto, through appropriate issuances and posting on its official website, and shall, where applicable, coordinate with the DBM, DOF, COA, and other concerned agencies prior to implementation, in accordance with existing laws, rules, and regulations. The Schedule of Fees shall be reviewed periodically and adjusted as necessary.

SECTION 13. ***Performance Scorecards, Compliance Certification, and Public Disclosure.*** —

(a) ***Performance Scorecards.*** The DICT shall develop, maintain, and periodically update a standardized E-Governance Performance Scorecard to assess the level of compliance of Covered Entities with the requirements of the Act, this IRR, and related DICT issuances. The Performance Scorecard shall be aligned with the EGMP, E-Government Development Index (EGDI), and applicable standards, and may include, among others, indicators on:

(1) compliance with prescribed ICT, interoperability, cybersecurity, and data privacy standards;

(2) implementation status of required E-Government Programs;

(3) quality, accessibility, and availability of digital public services;

(4) institutional readiness, including governance, human capital, and ICT planning; and

(5) timeliness and accuracy of required reports and submissions to the DICT.

The Performance Scorecards shall only be advisory in nature.

(b) ***Certification of Compliance.*** Based on validated submissions from Covered Entities, and audits, assessments or monitoring activities, the DICT may issue the following certifications:

(1) Certificate of Compliance, indicating that a Covered Entity has substantially complied with applicable requirements, standards, and timelines under the Act, this IRR, and relevant DICT issuances; or,

(2) Certificate of Non-Compliance, indicating material gaps, deficiencies, or failures to comply with required standards, obligations, and corrective actions and compliance timelines, when necessary. Prior to issuance of such Certificate of Non-Compliance, DICT shall provide the Covered Entity a written notice of findings and a period of not less than fifteen (15) working days upon receipt of notice to respond with corrective actions or clarifications.

(c) ***Publication and Transparency.*** Subject to applicable laws on data privacy, confidentiality, and national security, the DICT may publish Performance Scorecards and any certifications issued to Covered Entities under this Section through official government websites, dashboards, or reports, for purposes of transparency, benchmarking, and public accountability.

RULE III
THE E-GOVERNMENT MASTER PLAN, PROGRAMS AND SYSTEMS

SECTION 14. ***E-Government Master Plan (EGMP).*** — The DICT shall formulate and promote an EGMP or its equivalent that will serve as a blueprint for the development and enhancement of all electronic government service processes and workforce to achieve digital transformation in the bureaucracy, taking into consideration the Philippine Development Plan. The EGMP shall serve as the sole and overarching national roadmap for the development, harmonization, and enhancement of all electronic government programs, systems, platforms, and digital services.

An Integrated Framework shall also be developed to provide the government enterprise architecture and operationalize the blueprint through programs and projects relating to E-Government, to fully realize the vision, goals, and objectives of the EGMP. The Integrated Framework shall also set forth the guidelines for the government Enterprise Architecture, and implementation roadmap to ensure coherence, efficiency, and alignment of all government ICT systems and platforms.

The EGMP and its integrated framework shall include core governance principles for the responsible deployment of emerging technologies, by mandating adherence to principles of transparency, accountability, and robustness in all E-Government programs. To ensure effective implementation of E-Governance, a whole-of-government approach shall be adopted in the formulation and promotion of the EGMP. This approach shall facilitate engagement primarily with government agencies, instrumentalities, GOCCs, LGUs, Regional Development Councils, ICT Councils, technical and standards organizations, and other relevant stakeholders to ensure the full and effective implementation of the country's E-Governance Agenda.

The DICT shall formulate, adopt, and publish the EGMP and its Integrated Framework within ninety (90) days from the effectivity of this IRR, and shall review and update the same every three (3) years or earlier as the need arises, in anticipation of disruptions, emergencies, crises, and new and emerging technologies.

SECTION 15. ***E-Government Programs.*** — The DICT, in coordination with relevant government agencies, shall develop the following programs and systems that will be regularly updated in consultation with stakeholders and ensure that such programs and systems are compliant with standards imposed by relevant laws, rules, and regulations relating to data privacy and cybersecurity. All E-Government Programs, platforms, and digital systems shall be designed, enhanced, and implemented strictly in accordance with the EGMP and shall comply with the PGIF. No E-Government Program shall introduce an independent framework,

architecture, roadmap, or standards regime inconsistent with, or supplementary to, the EGMP or PGIF.

To carry out the objectives of the Act, the DICT may develop or adopt additional E-Government Programs, platforms, or digital systems as may be necessary, subject to the same requirements on alignment with the EGMP, compliance with the PGIF, and adherence to applicable data privacy, cybersecurity, and information security standards.

The President of the Philippines may require Covered Entities to utilize the platforms established by the DICT; Provided, That nothing in this section shall be construed to derogate from the fiscal and administrative autonomy of government agencies, offices, and instrumentalities granted by law.

SECTION 15.1. ***Citizen Frontline Delivery Services Platform (CFDSP).*** — Within ninety (90) days from the effectivity of this IRR, the DICT shall issue and publish the minimum standards for integration into the CFDSP, currently known as the eGovPH Application (eGovPH SuperApp). These standards shall define the technical, operational, and interoperability requirements necessary for government systems to securely and efficiently connect to the Platform.

Covered Entities, with frontline services, shall be required to establish and maintain an information system dedicated to the delivery of their respective frontline services. Such systems shall enable citizens to access, request, and track frontline transactions electronically and shall conform to the minimum standards set by the DICT.

Covered Entities that already operate existing information systems or digital platforms for frontline services shall, within one hundred eighty (180) days from the effectivity of the rule prescribing minimum standards, file an application for integration with the DICT to connect to the eGovPH SuperApp.

Covered Entities that do not yet have an operational information system for frontline delivery shall, within the same one hundred eighty (180) day period, include the development and deployment of such a system as a priority project in their respective ISSPs, to be submitted to and approved by the DICT and DBM. The ISSP shall outline the implementation timeline, funding requirements, and institutional arrangements necessary for integration into the eGovPH SuperApp.

Pending the development of a full information system, Covered Entities shall at least maintain an official website capable of publishing public information, downloadable forms, and clear instructions for accessing frontline services. This website shall comply with DICT's web, accessibility, and cybersecurity standards, and shall serve as the initial entry point for future integration into the eGovPH SuperApp.

The DICT shall monitor and evaluate agency compliance with these requirements and may issue technical advisories, compliance directives, or non-compliance notices as necessary. The DICT shall periodically review and update the minimum standards to reflect emerging technologies, evolving interoperability needs, and international best practices.

SECTION 15.2. ***Electronic Local Government Unit (eLGU) System.*** — Within one (1) year from the effectivity of this IRR, the DICT and Department of the Interior and Local Government (DILG) shall develop, adopt, and publish a Local Government Digital Service Standard (LGDSS) that shall define the minimum set of digital public services which all LGU systems or portals must provide. The LGDSS shall serve as a uniform benchmark to ensure consistency,

accessibility, interoperability, and efficiency in the delivery of local digital services across all levels of local governance. At a minimum, the LGDSS shall cover business and investment-related services, such as the processing of business permits, clearances, and licenses; revenue and taxation services, including assessment and payment of real property tax, business tax, and other local fees; civil registry services, including applications and issuances related to birth, marriage, and death certificates; citizen request and feedback mechanisms; and other frontline services as may be determined by the DICT, the DILG - Bureau of Local Government Development, and the Department of Finance (DOF) - Bureau of Local Government Finance (BLGF), consistent with the LGU's Citizen's Charter, the EODBA, and other applicable laws, rules and regulations.

LGUs that opt to develop, maintain or utilize their own eLGU systems or portals must demonstrate full compliance with the LGDSS as a prerequisite for certification and recognition by the DICT. Such LGU-utilized systems shall undergo technical validation by the DICT to ensure full interoperability and API-based integration with the national CFDSP, compliance with applicable data privacy, cybersecurity, and interoperability standards prescribed under the EGMP, and adherence to user-centered design and accessibility standards consistent with international best practices. For systems involving revenue generation, the validation shall be conducted in coordination with the BLGF to ensure compliance with fiscal policies.

Only those LGUs certified as fully compliant with the LGDSS and integrated with the eGovPH SuperApp shall be deemed compliant with the requirements of the Act and this IRR. LGUs that fail to establish or integrate compliant systems within the prescribed period shall be required to fully adopt the DICT-provided eLGU system, for which the DICT shall provide the necessary software, infrastructure, and technical assistance to ensure continuity of digital services to the unserved or underserved municipalities.

The DICT shall periodically review and update the LGDSS at least once every two (2) years from the effectivity of this IRR, or as necessary to reflect technological advancements, user feedback, and evolving digital governance priorities.

SECTION 15.3. ***Government Digital Payment System for Collection and Disbursement.*** — An electronic payment facility and gateway that will enable citizens and businesses to remit and receive payments electronically to or from government agencies shall be created. It shall render services through various delivery channels, which include debit instructions (ATM accounts), credit instructions (credit cards), and mobile wallets (mobile applications/SMS). For this purpose, the government may, in accordance with applicable laws and rules, engage the services of, and interconnect with, public and private payment systems and facilities, among others, consistent with the National Retail Payment System Framework of the Bangko Sentral ng Pilipinas (BSP).

These systems should interface smoothly with the current monitoring and accounting systems of the National Treasury.

Covered Entities are hereby encouraged to adopt and utilize the Government Digital Payment System currently known as "eGovPay" as established by the DICT for the electronic collection and disbursement of government payments. Covered Entities that have previously implemented or currently maintain their own digital or electronic payment platforms may continue to operate such systems; Provided, That they shall ensure full technical interoperability and secure interconnection with E-Government Programs, platforms, and services, including those under the EGMP. For purposes of alignment and integration, all Covered Entities shall coordinate with the DICT to facilitate system interconnection, integration, and compliance with standards.

The technical standards, implementation protocols, and operational guidelines governing the Government Digital Payment System shall be jointly formulated and issued by the DICT, the Bureau of the Treasury (BTr), the DOF-BLGF and the COA, consistent with their respective mandates, and shall be promulgated within one hundred twenty (120) days from the effectivity of this IRR to ensure uniform adoption, transactional integrity, audit compliance, transparent monitoring, real-time reconciliation, and seamless interconnectivity with government treasury systems, accounting platforms, and the whole-of-government digital payment ecosystem.

SECTION 15.4. ***Government Public Key Infrastructure (PKI) Program.*** — The DICT shall encourage and promote the use of Government PKI digital certificates that allow paperless transactions and remote approval by signatories in the government to reduce red tape and enforce ease of doing business. The adoption of PKI aims to strengthen E-Government cybersecurity through its implementation in all government offices and supply of digital certificates to the citizens. The Government PKI Program known as the Philippine National PKI (PNPKI) shall serve as the official Government PKI system that issues PKI digital certificates to ensure the security of digital data and transactions by providing:

(a) Authentication- to verify the identity of users and prevent unauthorized access to information and systems;

(b) Confidentiality- to ensure that electronic data and communications are accessible only to authorized parties;

(c) Integrity- to ensure that electronic data and messages remain complete, accurate and unaltered during transmission and storage; and

(d) Non-repudiation- ensure that parties to an electronic transaction cannot deny their participation or actions.

Within ninety (90) days from the effectivity of this IRR, the DICT shall issue the guidelines on the use of PNPKI Systems and accreditation of Registration Authority and Government Certificate Authority, establishing the policies, technical standards, and accreditation framework necessary for the secure implementation of PKI across the government.

All Covered Entities shall, as far as practicable, ensure that their employees, especially those authorized to approve, certify, or endorse documents or transactions, are enrolled in or have access to the Government PKI system.

SECTION 15.5. ***Human Capital Management Information System (HCMIS).*** — An HCMIS shall be developed to eliminate paper-based and manual human resource (HR)-related processes. Consistent with applicable civil service laws and rules, the HCMIS shall automate the following HR-related functions in government: recruitment and selection, appointment preparation and submission, personnel records keeping, salary, benefits, and payroll administration, leave management, learning and development, rewards, recognition, and performance management, among others. This system shall utilize analytics to provide insights necessary for strategic HR functions such as performance management, forecasting, promotion, succession planning, among others; Provided, That government agencies, offices, and instrumentalities granted by law and their respective charters with fiscal and administrative authority in the performance of their constitutional and statutory mandates, including those that have been exempted from the Salary Standardization Law and have been granted authority to formulate their own classification systems, shall be allowed to independently develop,

maintain, undertake, supervise, and regulate their own HCMIS and shall be required to coordinate and report to the DICT for alignment of policy objectives.

Covered Entities are encouraged to adopt and utilize the national HCMIS established pursuant to this IRR, subject to system readiness and capacity of the concerned agency. The DICT and CSC may utilize, co-develop, and enhance the existing HCMIS of the CSC provided it complies with the minimum standards defined under the Act and this IRR. The CSC and the DICT shall jointly issue and promulgate the minimum technical, data governance, cybersecurity, and operational standards for system implementation and integration within ninety (90) days from the effectivity of this IRR. Compliance with these standards shall be mandatory for all HCMIS implementations across government, without prejudice to enhanced system features adopted by agencies consistent with their mandates.

SECTION 15.6. ***Integrated Financial Management Information System (IFMIS).*** — To ensure fiscal discipline, fund allocation efficiency, and operational efficiency in the delivery of public services, an IFMIS shall be jointly developed by the DBM, DOF, COA, and DICT. This shall harmonize all existing financial systems in government to enable real-time, online accounting monitoring, and control of obligations and disbursements and directly link these to cash management for a more effective financial control and accountability. This shall facilitate the generation and monitoring of vital information on all aspects of government financial transactions to support timely and informed decisions across the bureaucracy.

Covered Entities are encouraged to adopt and utilize the IFMIS established pursuant to the law and this IRR, subject to system readiness and capacity of the concerned agency. The DICT and CSC may utilize, co-develop, and enhance the existing IFMIS of the DBM provided it complies with the minimum standards defined under the law and this IRR. The DBM, DOF, COA, and DICT shall jointly develop and promulgate the minimum technical, cybersecurity, data governance, and operational standards for IFMIS implementation within ninety (90) days from the effectivity of this IRR.

SECTION 15.7. ***Integrated Government Network (IGN).*** — Covered Entities that maintain existing internal or legacy networks, or those operating networks pursuant to their respective charters with fiscal and administrative authority, may continue to independently develop, operate, and maintain such networks; Provided, That they ensure continuing interoperability with the IGN, comply with national cybersecurity and information security standards, and submit network interoperability compliance reports to the DICT for policy and Enterprise Architecture alignment.

Covered Entities are encouraged to adopt and utilize the IGN once operational.

The DICT shall issue the guidelines for the operation, use, management, resiliency, incident response, and administration of the IGN, including the governance of the Government Internet Protocol Exchange (G/IPX) Facility, within one hundred twenty (120) days from the effectivity of this IRR.

For purposes of this IRR, the IGN will cover the following:

(a) the orderly turnover, integration, and transition of the existing Government Internet Protocol Exchange (G/IPX) facilities into the IGN architecture, including the mandatory connection, interconnection, or peering of all relevant government agencies and government networks to the designated G/IPX, consistent with the interoperability and unified traffic exchange framework for government networks;

(b) the establishment and operationalization of a Network Information Center (NIC) within the DICT to administer, manage, allocate, secure, and maintain all government IP resources;

(c) the acquisition, administration, and management of IP address blocks, internet number resources, and related allocations from APNIC and other authorized global numbering registries;

(d) the mandatory adoption and phased migration to the latest Internet Protocol versions, secure DNS and domain name administration standards for the .gov.ph domain, and the deployment of modern cryptographic protocols, including but not limited to TLS and SSL, to strengthen network resiliency and cybersecurity posture across all government entities; and

(e) formal and sustained coordination, engagement, and collaboration with internet governance bodies such as The Internet Corporation for Assigned Names and Numbers, Internet Assigned Numbers Authority, Asia Pacific Network Information Centre, and other international organizations to ensure alignment with internationally recognized norms, protocols, and best practices in resource management and interoperability.

The DICT, in coordination with the DBM, shall jointly issue guidelines, policies, and budgeting frameworks to optimize, rationalize, and harmonize government ICT expenditures. Such issuance shall provide direction on cost-efficient procurement, consolidation of duplicative ICT investments, prioritization of whole-of-government shared services, and alignment with the IGN.

The DICT shall promulgate supplemental technical guidelines, certification requirements, implementation schedules, interoperability specifications, compliance mechanisms, and other necessary regulatory issuances to fully operationalize the IGN and to ensure secure, efficient, scalable, future-proof, and standards-aligned interconnection across all government networks and platforms, consistent with evolving global internet governance principles and emerging technologies. The operation of the IGN and the NIC shall be subject to periodic independent technical, cybersecurity, and information security audits, in accordance with standards prescribed by the DICT.

SECTION 15.8. ***Online Public Service Portal.*** — Complementing the CFDSP, an Online Public Service Portal shall be made accessible through digital platforms such as the internet and other ICTs to citizens of the Philippines; foreign nationals who have been lawfully admitted to the country; and businesses organized and existing or operating under the laws and rules of the Philippines for purposes consistent with efficient delivery of public services. The Online Public Service Portal shall serve as a help desk where citizens can request for information and assistance on government frontline services, service procedures, and report commendations, appreciation, complaints, and feedback.

For purposes of interoperability, interconnection, and harmonization, all existing systems or mechanisms, such as the 8888 Citizens' Complaint Center and government social media channels, established and/or maintained by government agencies, offices, and instrumentalities, and LGUs shall be integrated to the Online Public Service Portal. Likewise, the Online Public Service Portal shall be fully integrated with the IGN and Records and Knowledge Management Information System for real-time updating of data and information.

To ensure that the public is served efficiently and expeditiously in accordance with the objectives of the Act, all Covered Entities are hereby mandated to cooperate and coordinate with each other and with the Presidential Management Staff (PMS) to ensure prompt action on

the concerns received through the Online Public Service Portal and associated communication channels.

Notwithstanding the provisions of the Act and this IRR, access and use of resources, information, and data through the portal shall be in accordance with the DPA, EODBA and all relevant laws, rules, and regulations on data and information privacy and pertinent rules on confidentiality of government information.

Within one hundred twenty (120) days from the effectivity of this IRR, the DICT, in coordination with the Anti-Red Tape Authority (ARTA), PMS, and other concerned agencies, shall issue the guidelines on the integration, operation, and case referral mechanisms of the Online Public Service Portal to ensure timely action, accountability, and seamless workflow orchestration of lodged public concerns.

SECTION 15.9 ***Philippine Digital Health System.*** — A comprehensive, integrated, interoperable, progressive, secure, and sustainable ICT system and framework shall be established to provide wide access to quality health information and services that promotes and ensures streamlined and safety-regulated delivery of digital health services to reduce inequalities and achieve universal healthcare and better health outcomes for every Filipino.

The DICT may utilize, enhance, or improve the existing digital health systems of the Department of Health (DOH) as foundational components of the Philippine Digital Health System; Provided, That any enhancement, modification, or integration undertaken by the DICT shall strictly comply with the minimum standards on interoperability, data privacy, cybersecurity, patient safety, and all other applicable regulatory requirements promulgated under this IRR.

Within one hundred twenty (120) days from the effectivity of this IRR, the DICT and the DOH shall jointly develop, issue, and promulgate the implementing guidelines, technical protocols, system enhancement standards, access conditions, and operational procedures for the utilization and improvement of DOH digital health systems.

SECTION 15.10. ***Philippine Government Interoperability Framework.*** — The Philippine Government Interoperability Framework (PGIF) establishes technical, and data and informational interoperability of government ICT systems necessary for an effective and efficient delivery of government services by ensuring a seamless operations and shared services of the Philippine government, between and among its various agencies, and their constituents.

The PGIF shall consist of the following components:

(a) Domain 1 - establishes the overall principles and key standards that would enable systems to communicate with one another through the linkage of ICT systems and services among government agencies. It shall include the Technical Standards Catalogue, which shall constitute a structured collection of standards, specifications, and guidelines for interoperability requirements.

(b) Domain 2 - establishes the common methodology, definition, and structure for data and information, along with shared services for its management throughout its lifecycle.

(c) Additional Domains - additional domain(s) that form part of the government interoperability may be developed or issued in the future for government wide application to ensure proper consolidation, coherence, and continuous updating of the framework and its technical standards.

All Covered Entities shall adopt and implement the PGIF in their ICT systems, projects, programs, and processes. The PGIF shall likewise apply to private entities that will participate as ICT solutions or service providers to the Philippine government, this includes, but not limited to, entities involved in the design, development, supply, operation, maintenance, management, or support of government ICT systems, applications, platforms, infrastructure, or data-related services. The DICT shall be the lead implementing and governing authority for the PGIF.

For this purpose, the DICT shall establish a PGIF Management Team, supported by a Technical and Sectoral Working Group, which shall be responsible for the overall policy direction, coordination, and oversight of government-wide interoperability initiatives. The DICT shall issue the necessary and relevant technical advisories and guidelines to operationalize the adoption of the PGIF. The PGIF shall be reviewed and updated regularly at least every two (2) years or earlier as necessary to ensure responsiveness to the current needs of the government and alignment with newly adopted standards and technological trends.

Covered Entities are required to submit annual implementation reports to the DICT for evaluation. These reports will serve as the basis for the continuous updating of interoperability guides, policies, and standards. All E-Government Program interoperability requirements and applicable ICT-related procurement, development, and modernization projects of all covered government agencies shall conform with the standards and requirements of PGIF, and the guidelines and standards for ISSP as determined by the DICT.

The DICT shall develop, promulgate, and formally issue the PGIF within one hundred twenty (120) days from the effectivity of this IRR.

SECTION 15.11. ***Procurement System.*** — A modernized Philippine Government Procurement System shall be developed and implemented to provide an auditable online system that encompasses all procurement and supply chain management processes involving bidding, contract management, delivery, acceptance, and payment for services or supplies: Provided, that government agencies, offices, and instrumentalities granted by law and their respective charters with fiscal and administrative autonomy in the performance of their constitutional and statutory mandates shall independently develop, maintain, undertake, supervise, and regulate their own procurement systems and shall only be required to coordinate and report to the DICT for alignment of policy objectives: Provided, further, That such system shall comply with the NGPA.

The DICT and DBM may utilize, co-develop, and enhance the existing PhilGEPS of the DBM provided it complies with the minimum standards defined under this IRR. The DICT, DOF, COA and DBM, shall jointly develop and issue the implementation guidelines within ninety (90) days from the effectivity of this IRR to ensure alignment, transparency, audit integrity, and whole-of-government readiness.

SECTION 15.12. ***Records and Knowledge Management Information System.*** — A Records and Knowledge Management Information System shall be designed to systematically and efficiently manage government documents, records, and knowledge products and services. This includes the digitalization of paper-based documents, records, and knowledge products and services, as well as the re-engineering and digitalization of paper-based workflows, from creation, dissemination, processing, analysis, tracking, storing, verification and authentication, and archiving or disposal, while adhering to existing policies, laws, and internationally recognized standards and best practices.

A repository and corresponding secure API shall be created for the common data sets, which include pricing, demographic, and geospatial data to improve publication, sharing, and utilization of data across the government. The DICT shall ensure that such repository shall be compliant with the DPA, its IRR, and relevant issuances of the NPC and information security standards. The DICT shall also establish a platform or its equivalent for government data storage and interoperability.

DICT, together with the National Archives of the Philippines, Philippine Statistics Authority (PSA), and other concerned agencies shall jointly develop and issue the implementation guidelines within ninety (90) days from the effectivity of this IRR to ensure alignment, transparency, audit integrity, and whole-of-government readiness.

The DICT, in collaboration with the relevant agencies, shall issue the necessary guidelines to accelerate the adoption of Open Data.

SECTION 16. ***National E-Government Development Index (EGDI).*** — The DICT, in coordination with other government agencies, shall establish a national EGDI to serve as the unified metric for assessing and monitoring the progress of E-Government development in the country. The EGDI shall provide a framework for internal assessment and external benchmarking against global standards.

The EGDI shall be the composite measure, consistent with international best practices, of the three important dimensions of E-Government, namely: online service index, telecommunication infrastructure index, and human capital index, and shall adopt globally competitive indicators, definitions, and statistical standards.

The EGDI shall be published every two (2) years from the effectivity of this IRR.

SECTION 17. ***Measurement Manual.*** — The DICT shall develop and publish an official E-Government Measurement Manual detailing the framework, indicators, computation methods and data collection procedures. The Manual shall adhere to internationally recognized standards such as the United Nations EGDI, Organisation for Economic Co-operation and Development Digital Government Index, International Telecommunication Union, and other global E-governance standards, and shall undergo consultation and validation by the member agencies of the Inter-Agency Committee on ICT Statistics, created by PSA Memorandum Order No. 12, series of 2015, and other stakeholders.

The Manual shall be reviewed and updated at least once every three (3) years from the effectivity of this IRR or as necessary to respond to the emerging technologies, global benchmarking practices, and policy priorities.

SECTION 18. ***Annual E-Government Maturity Survey.*** — The DICT shall conduct an annual E-Government Maturity Survey to assess the ICT readiness and digital maturity of Covered Entities based on the framework established by the National EGDI, with focus on the following: digital service delivery or the extent of services migrated online; efficiency of ICT management; human resource capacity; adherence to information security standards; citizen engagement and accessibility; and, compliance to the principles and standards of the PGIF.

Participation in the annual E-Government Maturity Survey shall be mandatory for all Covered Entities.

The results of the annual E-Government Maturity Survey shall be the primary basis for the mandatory three (3) year review and update of the EGMP, ensuring the national strategy is responsive to performance data

The survey results, including individual agency scores and rankings, shall be published on a public dashboard. Agency performance in this survey shall be a mandatory criterion in the annual performance evaluation of the head of the Covered Entity and the CIO.

SECTION 19. ***Free Access to the Internet for the Public.*** — Subject to compliance with existing laws, rules and regulations, the Free Public Internet Access Program shall utilize the Free Public Internet Access Fund (FPIAF) to finance capital outlay, maintenance and operations of the program, and to provide necessary computer systems, programs, databases, management and information systems, and core transmission and distribution networks to facilitate knowledge-building among citizens and empower them to participate in the evolving digital age.

The provisions of R.A. No. 10929 or the "Free Internet Access in Public Places Act" and its implementing rules and regulations shall be suppletory to the Act and this IRR.

RULE IV
GOVERNMENT WEBSITE AND INFORMATION PORTALS

SECTION 20. ***Government Website and Electronic Bulletin (E-Bulletin) Board.*** — Covered Entities are mandated to set up, maintain, and consistently enhance their websites and to establish an e-Bulletin Board for efficient information dissemination. This mandatory enhancement shall be aligned with the strategic objective of consolidating the government's digital presence through the eGovWeb platform. The website and e-Bulletin board should be interactive, well-designed, functional, and mobile-friendly, operating on a secure foundation prioritizing cybersecurity and accessibility. Government websites shall be updated regularly.

To guarantee platform resiliency and secure interoperability, the DICT, in coordination with relevant agencies, shall promulgate supplemental technical standards and implementation guidelines for website modernization and e-Bulletin Board establishment within ninety (90) days from the effectivity of this IRR. These guidelines shall mandatorily include detailed cyber hygiene requirements for all government digital assets to be integrated with the eGovWeb platform.

SECTION 21. ***Minimum Standards for Government Websites.*** — The following minimum standards shall apply to government websites and information portals:

(a) must contain direct and easily identifiable links to: (i) description of the mission, statutory authority, and the organizational structure of the agency; and (ii) frequently asked questions (FAQs) with the corresponding answers, and other common matters of public concern; and (iii) portals of relevant and applicable E-Government Programs for public service delivery;

(b) must provide access to public information via an API;

(c) subject to compliance with the DPA, must include up-to-date government directory containing the contact information, such as emails and telephone numbers, of the offices and officials of the Covered Entity;

(d) must comply with the Philippine Web Accessibility policy, or any relevant issuance from the DICT;

(e) must provide a real-time citizen feedback mechanism integrated into all E-Government platforms to allow users to rate services, provide comments, and report issues directly. Data from this mechanism shall be publicly aggregated and published quarterly to ensure transparency and guide service improvements;

(f) must include procurement-related notices and monitoring platforms, in compliance with NGPA, and

(g) must provide information on website owner contact, hosting provider, and agency CISO/CSIRT contact to the NCERT for coordination in case of a cybersecurity incident.

SECTION 22. ***Information Dissemination through Website and E-Bulletin Board.*** — Covered Entities shall publish public notices, documents, or information on their websites, e-Bulletin boards, and verified official government social media accounts, in addition to traditional publication methods.

Except when a different manner of publication for effectivity is required by other laws, publication on the official government website and E-Bulletin Board shall be deemed sufficient legal notice, and the date and time of posting thereof shall serve as the official reference point for reckoning publication.

RULE V
ROLE OF COVERED ENTITIES AND THEIR RESPECTIVE HEADS

SECTION 23. ***Responsibilities of Heads of Covered Entities.*** — The head of each Covered Entity, in consultation with the DICT, shall:

(a) ensure adherence to requirements of the Act, this IRR and all other laws including relevant DICT issuances on standards for all ICT infrastructure, systems, equipment, designs, and technologies;

(b) ensure compliance with the standards and protocols for cybersecurity, resiliency, data privacy and confidentiality, as prescribed in relevant laws, rules, and regulations;

(c) ensure prompt and effective communication of ICT standards promulgated by the DICT to all concerned agency officials;

(d) support national and local government efforts and, where appropriate, collaborate to develop, maintain, and promote an integrated system for delivering government information and services to the public;

(e) ensure the establishment and implementation of policies and standards on cybersecurity, freedom of information, and open data within their organization following its mandate and technological needs or risks;

(f) comply with the re-engineering and streamlining requirements of the ARTA as provided under the EODBA; and

(g) ensure continued availability of government information and services to all individuals and entities, including those without internet access, through accessible alternative delivery channels, whether electronic or manual.

SECTION 24. ***Responsibilities of Covered Entities.*** — To achieve the objectives of the Act and this IRR, Covered Entities shall:

(a) adopt policies, procedures, standards, and guidelines that are in accordance with law and as directed by the President of the Philippines;

(b) develop performance measures that demonstrate how ICT advances agency objectives, statutory mandates, and strategic goals aligned with key stakeholders, including citizens, businesses, and other governments;

(c) guide policies and programs, collect and analyze relevant data including on customer service, productivity, and the adoption of innovative information technology in accordance with industry best practices;

(d) as appropriate, work collectively in linking their performance goals to key groups and use information technology in delivering government information and services to those groups;

(e) take necessary measures to prevent algorithmic bias or discrimination, particularly in the use and deployment of emerging technologies, that could compromise the inclusivity and equity of access to government services;

(f) maintain and update their websites and e-bulletin boards in accordance with the standards set by the DICT;

(g) submit EA, ISSPs and ICT plans, and such other mandatory plans and reports within the timelines prescribed in this IRR and other relevant issuances;

(h) update ISSPs and ICT plans annually, integrate them into budget planning, and be accountable for their implementation;

(i) regularly undertake cost compliance analysis, time and motion studies, undergo evaluation and improvement of their transaction systems and procedures and re-engineer the same if deemed necessary to reduce bureaucratic red tape and process time; and,

(j) support the development of a digital competency framework to undertake a competency assessment of personnel and provide them with appropriate learning and development programs to strengthen their digital competency.

SECTION 25. ***Responsibilities as regards Data Security and Privacy.*** — Covered Entities shall comply with the standards and protocols for cybersecurity, resiliency, data privacy and confidentiality, as prescribed in relevant laws, rules, and regulations. To this end, Covered Entities shall:

(a) establish and implement policies and standards on information security, freedom of information, and open data within their organization following its mandate and commensurate with its risk profile and the magnitude of the potential harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected, stored,

processed or maintained by or on behalf of the agency; and information systems used or operated by an agency, its contractor, or by other organizations on its behalf;

(b) ensure that all E-Government Programs comply with the data subject rights, security and data protection requirements of the DPA, and shall formally seek and incorporate guidance and assistance from the NPC on matters concerning information security and protection of personal data;

(c) comply with the Minimum Information Security Standards (MISS) set by the DICT, and submit proof of compliance thereof in accordance with Section 38 of this IRR;

(d) periodically test and evaluate information security controls and techniques to ensure that they are effectively implemented;

(e) integrate information security management processes with agency strategic and operational planning processes;

(f) adopt the Privacy-by-Design, Privacy Engineering, and Privacy-by-Default principles by implementing the measures in developing, implementing, and deploying systems, processes, software applications, and services throughout the personal data processing lifecycle, in accordance with the relevant guidelines issued by the NPC; and,

(g) allocate resources necessary to implement cybersecurity and data protection measures set in this Act, IRR, and other relevant issuances of the DICT.

All Covered Entities shall be responsible for the security, integrity, and lawful processing of information within their information systems, whether such systems are operated by the Covered Entity itself, or by a contractor or third-party on its behalf. In the event of a breach of personal data, the failure to uphold these responsibilities may be construed as evidence of negligence under the DPA.

SECTION 26. ***Liability of Heads of Covered Entities.*** — The heads of Covered Entities shall be primarily responsible for ensuring compliance by their respective agencies with the Act and this IRR, and non-compliance thereto may subject them and other responsible officers to sanctions and penalties under the Administrative Code of 1987, as amended, the Revised Rules on Administrative Cases in the Civil Service, EODB, and other applicable laws, rules, and regulations.

SECTION 27. ***Review of Existing Policies, Programs and Standards.*** — With the assistance of DICT, all Covered Entities shall review all their policies, programs, standards, and relevant contracts and agreements, including on the operation of related ICT infrastructure, systems, equipment, or services, to ensure compliance and alignment with the Act and this IRR.

When necessary, Covered Entities shall upgrade, enhance, reconfigure or replace their existing systems, standards, protocols, mechanisms, equipment, programs, or infrastructure, and negotiate with their respective counterparties to amend, modify or supplement relevant agreements, to ensure compliance with the provisions of the Act, this IRR and other issuances on MISS, cybersecurity protocols, and data privacy requirements. These must be completed within the period prescribed by the DICT, taking into consideration the system's nature, criticality, and operational impact, and procedures under prevailing laws.

For purposes of efficiency and avoidance of redundancy, Covered Entities with existing: (i) standards for all ICT infrastructures, systems, equipment, designs, and all other technology;

(ii) protocols for cybersecurity, resiliency, and data privacy and confidentiality; (iii) mechanisms for communicating promptly and effectively all information technology standards within their agency; and (iv) equipment, systems, programs, and infrastructure that substantially comply with the minimum requirements, as determined by the DICT, shall be deemed compliant with the provision of the Act and this IRR, and shall be allowed to maintain those existing standards, protocols, mechanisms, equipment, systems, programs, infrastructure, and positions. Contracts for such existing projects and programs deemed compliant shall remain valid until expiration or termination thereof.

SECTION 28. ***Guidelines on Privacy Engineering in Systems Life Cycle Processes.*** — Covered Entities shall observe the following guidelines throughout all phases of the system lifecycle.

(a) Planning and requirements gathering

(1) Determine the lawful basis for processing personal data, and ensure that the purpose, scope, and manner of processing are compatible with the declared and specified purpose;

(2) Apply the general data privacy principles of transparency, legitimate purpose, and proportionality in collecting personal data. Agencies should only collect data that is adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose, and retain it only for a specified period to fulfill that purpose or as required by law; and

(3) Conduct a (PIA) to identify and evaluate the potential risks and effects that the proposed data processing system may have on the data subjects, and to identify ways in which any adverse effects can be mitigated.

(b) Designing and development

(1) Minimize the processing of personal data by implementing architectures, practices, and techniques that reduce the use, collection, and retention of personal data to what is necessary in relation to the specified purpose;

(2) Implement appropriate information security measures to maintain the confidentiality, integrity, and availability of personal data;

(3) Implement measures within the system for data subjects to exercise their rights under the DPA, such as but not limited to: data access and download tools to request access to their personal data within the system; correction and rectification interfaces that allow users to rectify incorrect personal data; deletion or erasure options, to allow users to delete data within the system; and provide opt-in and opt-out mechanisms for specific processing of personal data;

(4) Maintain traceability in the data processing system involving access or changes made to personal data;

(5) Adopt secure software development practices that integrate privacy considerations throughout the systems life cycle processes;

(6) Establish data retention policies that define how long personal data can be stored, (e.g., use of temporal data), where collected data is regularly deleted after usage; and

(7) Implement secure disposal procedures and practices to ensure personal data is permanently deleted when it is no longer needed.

(c) Testing and evaluation

(1) Perform data privacy and information security testing to verify the effectiveness of the security and privacy controls and settings of the data processing system before deployment;

(2) Test the usability of the privacy interfaces, such as the accessibility of privacy notices that are clear and understandable and testing the mechanism on how data subjects can easily exercise their privacy rights through the system;

(3) Conduct code reviews and vulnerability scans to identify and address any information security flaws and weaknesses that can lead to unauthorized access and data breaches; and

(4) Conduct a privacy architecture review to ensure that technologies, architectures, and protocols used in the data processing system support data privacy objectives and requirements of the DPA, and issuances of the NPC.

(d) Deployment and integration

(1) Provide data subjects with clear and concise privacy notices regarding the collection and processing of their personal data, including their rights and how to exercise them. For example, users should be informed about the data that an application or a data processing system will be processing. Avoid deceptive design patterns to ensure transparency and trust. This approach not only delivers clear privacy notices but also enhances the overall trustworthiness of data processing systems;

(2) Obtain the proper consent of data subjects, when consent is the lawful basis for processing, before collecting and processing their personal data; and

(3) Ensure that the default settings of the data processing system provide the maximum privacy protection without manual intervention from data subjects. Some examples include, but are not limited to the following: the security settings of a system should be enabled by default; online forms only require essential information by default and leaving optional fields unrequired; opt-in consent mechanism by default with unchecked consent boxes; default user profiles should be private rather than public; location tracking should be disabled by default; and payment details should not be saved by default.

(e) Operation and maintenance

(1) Regularly monitor the data processing system for any information security incidents and data breaches, and implement policies and procedures for incident response and breach notification;

(2) Conduct periodic audits and PIAs at least once a year to assess the continued effectiveness of the privacy controls and address any gaps or new risks; a new PIA must be conducted in case of the following: (i) a major update or

enhancement to an existing system is made; (ii) a new vendor or third party processor is engaged; and (iii) changes in the nature, scope, extent, or purpose of processing;

(3) Promptly address any vulnerabilities and update the privacy controls of the data processing system based on the latest risks and information security standards;

(4) Uphold the requests of data subjects in exercising their rights (e.g., right to access, rectify, object, etc.) in accordance with the DPA, and the NPC's issuance on Data Subjects' Rights; and

(5) Train personnel on the secure processing in the application or data processing system, as well as managing information security incidents as stipulated in the DPA, and the NPC's issuance on managing information security incidents.

These measures shall apply regardless of the system's phase or status, whether newly developed, currently operational, or undergoing updates.

SECTION 29. ***Appointment and Institutionalization of the Chief Information Officer (CIO).*** — In accordance with the mandate of this Act to professionalize and elevate the government's digital leadership, all Covered Entities shall establish the CIO position, and for this purpose, coordinate with the DBM to cause the creation, classification, and funding of a plantilla position.

The CIO shall occupy a senior, executive, strategic-level rank situated not lower than two (2) levels from the Head of the Covered Entity to ensure authority in driving institutional ICT modernization and digital transformation. The CIO shall report directly to the Head of the Covered Entity or to the second highest official specifically designated to oversee the entity's digital transformation and ICT Portfolio. In accordance with DBM rules and regulations, the salary grade (SG) of the CIO shall be commensurate to the size of the ICT organizational unit that he/she will head and contingent upon the complexity and scale of the covered entity's approved Information Systems Strategic Plan (ISSP).

The DICT, the CSC, and the DBM shall jointly issue the guidelines for the creation of a plantilla CIO position in all Covered Entities within 120 days of the effectivity of the IRR to conform with existing standards, rules, and regulations. Such guidelines shall include, but not be limited to: (i) the criteria for tier classification and SG assignment for all Covered Entities, including local government units (LGUs); (ii) minimum educational and professional qualifications; (iii) mandatory competency and domain proficiency standards; (iv) ISSP alignment, approval, and reporting mechanisms; and (v) cybersecurity, data privacy, and information security compliance obligations of the CIO.

To ensure fiscal sustainability, the creation of the CIO position shall be facilitated through the abolition of the existing vacant or redundant positions within the current staffing pattern of the Covered Entities. Covered Entities with no vacant plantilla positions shall submit their requests for the creation of said position to the DBM for review and approval. The DBM shall evaluate the requests to ensure consistency with the Covered Entities' existing established organization, staffing, position classification, and compensation rules and regulations.

Pending creation of the plantilla position for the CIO and appointment of a qualified person thereto, Covered Entities may designate senior officials or ICT technical managerial personnel with relevant educational and professional background, and certifications in Project Management, Program Management, Technology Management, IT Service Management, Enterprise Architecture, Information Security, Data Privacy, and Risk Management, Data

Analytics, and ICT financial planning and budgeting, among others, or their respective representatives to the CIO Council, as their interim CIO.

The creation of organizational units and CIO positions in the LGUs shall be subject to the Local Government Code of 1991 and the pertinent CSC and DBM policies, rules, and regulations for this purpose.

SECTION 30. ***Functions of the Chief Information Officer (CIO).*** — The CIO shall be responsible for managing and implementing the ICT systems of the Covered Entity and shall ensure development and implementation of the agency's ICT plan, its security and compliance with DICT-prescribed standards, relevant laws, rules, and regulations, including the DPA. The CIO shall perform the following functions:

(a) serve as the primary accountable official for institutional digital transformation, managing operational ICT risks, system integrity, data governance, interoperability compliance, and alignment of ICT procurements with national standards and audit requirements, within the Covered Entity;

(b) advise agencies on how to leverage ICTs to optimize the delivery of secured public services and achieve efficient and cost-effective operations;

(c) securely develop, maintain, and manage the agency's information systems;

(d) manage and supervise the implementation of ICT-related projects, systems, and processes;

(e) ensure that the ICT systems and business processes are interoperable by design, enabling seamless integration and data exchange across the whole government digital ecosystem in accordance with national E-Governance standards;

(f) formulate and implement processes in relation to the adoption of ICT-based solutions, including emerging technologies as provided in the EGMP;

(g) facilitate the secure, automated, and proactive exchange of authorized datasets among government agencies in accordance with E-Governance standards;

(h) manage operational risks related to ICT, in coordination with the agency's management, CERT, and stakeholders, and a government CII's CISO, and integrate risk management into the planning process;

(i) ensure that the ICT programs and operations are consistent with national policies and prevailing industry standards;

(j) accelerate the adoption of open data, blockchain, and emerging technologies, while benchmarking against ICT industry best practices in ICT programs and operations;

(k) oversee the development, implementation, and maintenance of all organizational, physical, and technical security measures for government information systems to ensure full compliance with the DPA and relevant issuances of the NPC;

(l) ensure the rigorous operational implementation of the Privacy-by-Design, Privacy-by-Default principles, and Privacy Engineering throughout the entire systems life cycle processes, in coordination with the agency's designated Data Protection Officer (DPO);

(m) ensure that E-Government Programs are accessible and inclusive to persons with disabilities, as far as practicable, in adherence to digital inclusion principles and relevant accessibility laws; and

(n) Coordinate with the EGov UPMO the status of implementation of their ICT programs and projects.

To ensure objectivity and auditability of the ICT systems and processes that the CIO oversees and manages, the CIO shall not be designated as the CISO and shall not exercise functional authority over CERT operations and information security assurances.

SECTION 31. ***Role of the Chief Information Officer (CIO) Council.*** — The CIO Council created pursuant to Section 13 of the DICT Charter shall support the individual CIOs in fulfilling their functions by providing the following:

(a) strategic and policy support in the implementation of ICT strategies, enforcement of technical standards and policies, and policy advocacy on issues related to ICT;

(b) operational and technical support in managing ICT systems and resources through shared knowledge and services; and

(c) human capital and professional support in managing the ICT workforce.

SECTION 32. ***Inclusivity.*** — In implementing policies and programs under the Act, heads of Covered Entities shall, to the extent practicable, ensure government information and services are accessible to all, including those without internet access.

RULE VI
SECURITY AND PRIVACY

SECTION 33. ***Data and Information Security.*** — All resources, information, or data stored in or transmitted through the government information systems and all networks interconnected to and interoperable with it, the portals, and websites shall be kept secure and free from interference or unauthorized access that can hamper or otherwise compromise the confidentiality, integrity, and availability of the ICT assets.

Access to and use of the resources, information, and data in the government information systems shall be limited to the government and its duly authorized officers and agents, in accordance with all relevant laws, rules, and regulations on data and information privacy and the pertinent rules on confidentiality of government information; Provided, That the data used by all concerned government agencies, offices, and instrumentalities with access to information systems and used data stored therein shall be destroyed or disposed of in accordance with acceptable standards and guidelines existing under the law for disposal of data upon fulfillment of its purpose.

Any person who shall knowingly commit an act which results in the compromise of the information security and integrity of the government information systems and all networks interconnected to and interoperable with it, to the detriment of the government and the public, shall incur criminal liability in accordance with the provisions of applicable and relevant penal laws.

SECTION 34. ***Master Data Management.*** —Within one hundred eighty (180) days from the effectivity of this IRR, the DICT, in alignment with the PGIF, and through a technical working group, shall establish a Master Data Governance Framework, which shall define the process for the governance, maintenance, and creation of master data sets that shall serve as the authoritative "single source of truth" for master data to be used in all government transactions and services, taking into consideration data accuracy, consistency, and reliability across various systems and platforms of different government agencies.

The DICT, in coordination with the PSA and other relevant government agencies, shall develop, concurrently with the Master Data Governance Framework, a comprehensive data dictionary to define and standardize all master data elements across government agencies to ensure uniform interpretation and use.

The parent agency shall act as the data steward, with the mandate to own, maintain, update, share, and protect the master data under its jurisdiction, while providing controlled access to other agencies through secure, standards-based mechanisms in alignment with the PGIF.

Inter-agency access to master data shall not diminish the parent agency's obligation to own, protect, secure, maintain and share its data.

In line with the "Once-Only principle," Covered Entities shall endeavor to achieve interoperability and facilitate seamless data sharing within two (2) years from the effectivity of this IRR, such that citizens and business entities shall not be required to resubmit information that already exists or whose data have already been collected and recorded by the parent agency of a certain master dataset; Provided, That this shall not apply when a covered entity must collect data necessary to verify the identity or legal personality of a citizen or business entity accessing the services of a government agency.

Each master dataset shall be governed by a unique reference or identifier, such as, but not limited to, the National ID number, Business Identification Number (BIN), or Land Parcel ID, to enable interoperability and prevent duplication. Data exchange shall be conducted through secure APIs aligned with the PGIF.

Covered Entities shall adopt a risk-based methodology and guidelines for data classification, as prescribed by the DICT. For this purpose, each agency shall conduct an annual inventory of all data under its custody and control and determine the potential harm that could result from a breach of its confidentiality, integrity, and availability.

Verified master data collected by a parent agency shall be exchanged and reused through a data exchange platform, such as eGovDX and its equivalent platform, developed by the DICT, taking into consideration the data classification and security level of the master data. The data exchange platform shall be periodically reviewed and updated to incorporate the most appropriate emerging technologies.

All activities pertaining to the governance, processing, maintenance, and sharing of master data shall comply with the DPA, EODBA and other applicable laws, rules and regulations.

SECTION 35. ***Privacy Impact Assessment (PIA).*** — The DICT and the concerned agency shall conduct a mandatory PIA, according to relevant NPC guidelines, on the existing as well as proposed systems for processing personal data included in the EGMP, to identify privacy risks

and establish the appropriate control framework in line with existing data privacy and cybersecurity standards.

The PIA should take into account the nature of the personal data to be protected, the personal data flow, the risks to privacy and information security posed by the processing, current data privacy best practices, the cost of security implementation, and the size of the organization, its resources, and the complexity of its operations.

The conduct of a PIA is intended to:

(a) identify, assess, evaluate, and manage the risks represented by the processing of personal data;

(b) assist the DICT in preparing the records of its processing activities, and in maintaining its privacy management program;

(c) facilitate compliance by the DICT with the DPA, and other applicable issuances of the NPC, by determining:

(1) its adherence to the principles of transparency, legitimate purpose and proportionality;
(2) its existing organizational, physical and technical security measures relative to its data processing systems; and
(3) the extent by which it upholds the rights of data subjects.

(d) aid the DICT in addressing privacy risks by allowing it to establish a control framework.

The PIA shall include the following:

(a) data inventory identifying:

(1) the amount and type of personal data held;
(2) list of all information repositories holding personal data, including location;
(3) type of media used for storing the personal data;
(4) risks associated with the processing of personal data; and
(5) processing operations for the entire personal data life cycle, from collection to disposal or destruction;

(b) a systematic description of the personal data being processed or to be processed, including the purposes for such processing, anticipated purposes, and their corresponding lawful bases;

(c) an assessment of the general data privacy principles in relation to the processing;

(d) a holistic assessment of the risks to the rights and freedoms of a data subject; and

(e) an assessment of risks to the confidentiality, integrity, and availability of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing.

In conducting a PIA, it is important that its results are properly supplemented by a report that includes information on stakeholder involvement, proposed measures for privacy

risk management, and the process through which the results of the PIA will be communicated to internal and external stakeholders. Where appropriate, representatives of civil society organizations should be involved as stakeholders.

The risks identified in the PIA must be addressed by the responsible agency through a Control Framework. The contents of a Control Framework shall take into account, among others, the following:

(a) Nature of the personal data to be protected;

(b) Risks represented by the processing, the size of the organization, and the volume of personal data being processed;

(c) Current data privacy best practices in a specific industry;

(d) Cost of information security implementation; and

(e) Purpose and extent of data sharing or outsourcing agreements and their attendant risks.

DICT shall consult the NPC prior to commencement of processing where the PIA indicates that the processing would result in a high risk in the absence of measures taken to mitigate the risk.

The PIA and its Control Framework shall be reviewed annually by the responsible agencies, or at the soonest practicable opportunity in the event of any of the following occurrences, such as (i) a major update or enhancement to an existing system is made; (ii) a new vendor or third party processor is engaged; or (iii) changes in the nature, scope, extent, or purpose of processing. The PIA need not be submitted to the NPC, but it shall be made available by the DICT or the responsible agency upon the NPC's request arising from investigations or compliance checks.

SECTION 36. ***Controls for Joint Personal Information Controllers (PICs) and Data Sharing.*** — In scenarios where an E-Government system involves multiple government agencies acting as Joint Personal Information Controllers (Joint PICs), particularly when implementing E-Government Programs requiring Government-to-Government (G2G) data sharing, the PIA shall be conducted jointly by all participating PICs. The PIA should be jointly signed off by the respective Heads of Agency and their designated DPOs, certifying their adherence to the requirements mentioned in the DPA and the NPC's issuances.

SECTION 37. ***Inter-Agency Data Sharing.*** — For purposes of implementing E-Government Programs, projects, systems, and services, Covered Entities may share government data among themselves in the performance of their lawful mandates to support interoperability, integrated public services, and efficient delivery of government programs.

The sharing of personal data among Covered Entities should be necessary, relevant, and proportionate to a legitimate government purpose duly documented in a PIA, subject to applicable data privacy, information security, access control, audit, and accountability requirements under existing laws, rules, and standards, and to the latest guidelines of the NPC.

The sharing of non-personal and common data sets among Covered Entities for official government purposes shall not require the execution of a Data Sharing Agreement (DSA), provided that such sharing complies with applicable government policies on data classification

and access restrictions appropriate to the nature and sensitivity of the data being shared.

The absence of a DSA shall not diminish or excuse Covered Entities from their obligation as responsible PICs for the protection, integrity, and proper use of the personal data being shared with them, including means through which the data subjects can exercise their rights. Furthermore, inter-agency data sharing may be subject to review by the NPC on its own initiative or upon a verified complaint by an affected data subject.

SECTION 38. ***Minimum Information Security Standards MISS Compliance.*** — All government agencies and their instrumentalities shall adopt the necessary policies, rules, and regulations to comply with MISS prescribed by the DICT, which shall be aligned with internationally accepted standards and relevant laws, rules, and regulations. Government agencies may adopt additional information security standards higher or more stringent than the prescribed, such as sector-specific standards, provided that such adoption remains consistent with the minimum standards set by the DICT.

The DICT shall publish a list of its prescribed MISS, including but not limited to the Philippine National Standards (PNS)/International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001 Information Security Management System (ISMS), National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 and its accompanying Security Publications (SPs), Center for Internet Security (CIS) Controls, European Union Network and Information Systems Directive 2 (EU NIS2), European Network and Information Security Agency (ENISA) Regulatory Framework, United Kingdom Cyber Essentials, or other future iterations and evolving approaches, ninety (90) days after the effectivity of this IRR.

The DICT shall have the authority to update the list of MISS, as it deems it necessary and appropriate.

All government agencies shall submit proof of their MISS compliance, such as a copy of their third-party cybersecurity certification or self-attestation form, to the DICT within one (1) year from the issuance of the MISS list.

The DICT Cybersecurity Bureau shall:

(a) provide standardized risk assessment and information security documentation templates necessary for the compliance of Covered Entities;

(b) issue a certificate of compliance to government agencies based on the requirements as defined in this Section and other future related issuances;

(c) in collaboration with the NPC, Cybercrime Investigation and Coordinating Center (CICC), other relevant government agencies, the academe, private sector, and civil society, provide the proper guidance, assistance, and training on cybersecurity standards and/or requirements to all Covered Entities.

In accordance with applicable MISS, where a system utilizes automated processing or AI-enabled tools, security controls shall extend to model and data risks, supply chain risks, access controls, monitoring, and incident response, commensurate with the system's role, criticality, and operational context.

SECTION 39. ***Protection of Government Critical Information Infrastructure (CII).*** — Consistent with the prevailing National Cybersecurity Plan, the DICT shall issue, within one

hundred twenty (120) days upon the effectivity of this IRR, policy, rules, and regulations on the following:

(a) Definition of government CII;

(b) Criteria for classifying government CII;

(c) Process for designating government CII;

(d) MISS for compliance by government CII;

(e) Mandatory establishment of a dedicated in-house Agency CERT/ CSIRT or engagement of a private Agency CERT/ CSIRT, to be headed by a CISO, for all government CIIs;

(f) Mandatory notification and reporting of major (or material) information security incidents affecting their institutions by government CIIs to their Sectoral CERT or their government regulator, if a Sectoral CERT is not available, within 24 hours from discovery; and escalation of the incident report to NCERT, if the Sectoral CERT or government regulator requires assistance in incident response;

(g) Implementation of VAPT and annual Risk and Security Assessment by all government CIIs; Provided, That, VAPT engagements for Government CII shall be performed by DICT-accredited providers that meet the DICT Trusted Assessment Provider (D-TAP) criteria and that VAPT reports shall be submitted to the NCERT and to the D-TAP registry, or D-TAP's equivalent; and

(h) Other cybersecurity standards, measures, protocols, and guidelines for the protection of government CII.

The CISO shall lead the agency's information security governance, risk management planning and implementation, compliance with information security standards, CERT/CSIRT operations, coordination with government agency's DPO on data protection issues, and material incident notification, reporting, and response. A CISO may be responsible for a single agency or a cluster of government CIIs.

A government CII may designate a Chief Operations Technology Officer, instead of or in addition to a CISO, as applicable and as required by its charter and other pertinent laws.

The DICT shall have the authority to update the definition, criteria for classifying, and process for the designation of government CII, including the shift to risk-based classification of CII, based on the prevailing National Cybersecurity Plan.

The DICT shall provide the proper guidance, training, and assistance necessary to enable Government CII to comply with the minimum cybersecurity standards and measures, as provided by the Act, this IRR, and other relevant issuances pertaining to information security and data protection.

Government CII shall be subject to periodic cybersecurity audits conducted by the DICT or DICT-accredited Cybersecurity Assessment Providers and Cybersecurity Posture Assessment Laboratory(ies), for the purpose of verifying compliance with the cybersecurity requirements prescribed in the IRR and by DICT issuances.

Nothing in this IRR prevents a government CII from implementing additional standards, or other standards higher or more stringent than the minimum set by the DICT, as it deems necessary.

SECTION 40. ***Public Service Continuity Plan (PSCP).*** — Consistent with the existing issuances of the National Disaster Risk Reduction and Management Council (NDRRMC) and the CSC, all ICT systems and infrastructure covered in the priority programs of the EGMP and ISSPs shall be included as part of the Public Service Continuity Plan (PSCP) of all government agencies and instrumentalities, to ensure the continuous delivery of essential agency functions, notwithstanding any emergency or disruption.

The plan must consider the following:

(a) Personal data backup, restoration, and remedial time;

(b) Periodic review and testing of the business continuity plan which takes into account disaster recovery, privacy, business impact assessment, crisis communications plan, and telecommuting policy, among others; and

(c) Contact information and other business-critical matters (e.g., electrical supply, building facilities, ICT assets).

The NDRRMC, CSC, Office of Civil Defense (OCD), and the DICT shall jointly develop, issue, and promulgate the policies, technical standards, implementation protocols, minimum requirements, and operational guidelines governing the inclusion of ICT priority programs under the EGMP, and agency-level ISSPs into the PSCP of all Covered Entities. Said guidelines shall provide a resilience framework to ensure uninterrupted public service delivery before, during, and after emergencies, institutional disruptions, cybersecurity incidents, critical information infrastructure failures, or force majeure events. The implementing guidelines shall be issued within ninety (90) days from the effectivity of this IRR, and shall thereafter be adopted and operationalized by all Covered Entities in accordance with their respective mandates and in compliance with all applicable laws, rules, and regulations.

RULE VII
PARTICIPATION OF THE PRIVATE SECTOR

SECTION 41. ***Government Cooperation with the Private Sector.*** — Nothing in this Act shall prevent the Covered Entities from entering into contracts, agreements, or partnerships with the private sector for the latter to provide various resources, assets, and services to the government which would aid or enhance compliance with the provisions of the Act and this IRR. Subject to accreditation requirements, when applicable, Covered Entities may engage private contractors to carry out ICT-related functions, including CERT and CISO responsibilities; Provided, That the Covered Entity remains primarily accountable for ensuring these tasks are performed in accordance with all applicable laws, rules, and standards.

To ensure inclusivity and accelerate access to E-Government Programs, Covered Entities may also enter into contracts with public telecommunications entities and data transmission industry participants to build and operate networks, and provide internet connection giving priority to underserved and unserved areas.

All contracts or agreements with the private sector pursuant to the Act and this IRR shall be subject to the laws and rules on public accountability, transparency and good governance,

and shall be executed in full compliance with applicable laws including, among others, the NGPA, and R.A. No. 11966 or the "Public-Private Partnership Code of the Philippines" (PPP Code).

RULE VIII
THE ICT ACADEMY

SECTION 42. ***Reorganization of the ICT Literacy and Competency Development Bureau and Strengthening the ICT Academy for E-Governance.*** — The DICT shall reorganize and restructure its ICT Literacy and Competency Development Bureau (ILCDB) into the ICT Academy, hereinafter referred to as the "Academy."

SECTION 43. ***Functions of the Academy.*** The Academy shall be the government's central institution for ICT Education, workforce upskilling, and E-Governance competency development.

The Academy shall have the following purposes and functions:

(a) serve as the National Center of Excellence for ICT Education;

(b) conduct trainings on E-Governance in furtherance of the Act and this IRR;

(c) promote ICT education to enhance the nation's workforce capacity, guided by up-to-date data on domestic and global skills supply and demand;

(d) promote and conduct quality ICT education for the capacity development of all citizens;

(e) support the strategic goals of the National ICT Development Agenda through data collection and globally competitive ICT skills development programs;

(f) implement programs and activities that will equip citizens with globally competitive skills and foster inclusive economic growth;

(g) establish partnerships with persons, entities, and institutions for the development and updating of resources, curriculum, modules, and pedagogical approaches;

(h) promote gender parity through technology education;

(i) ensure continuous learning and professional development for educators in current ICT trends;

(j) promote internships, immersion, apprenticeships, and other enterprise-based trainings for learners with industry partners, both private and public;

(k) establish and implement a scholarship system for qualified individuals in training and programs under the Academy or other activities approved by the DICT Secretary;

(l) facilitate the screening, admission, and monitoring of scholars within the scholarship system under Section 43(k);

(m) undertake academic research and development related to ICT;

(n) regularly assess the state of the country in terms of comparative ICT skills and performance and propose responsive policies to address concerns;

(o) develop curricula and courses for learners and students to upskill ICT proficiency and competency, and to ensure that such curricula and courses are aligned with its relevant competency frameworks through consultations and collaborations with the Commission on Higher Education (CHED), Department of Education (DepEd), Technical Education and Skills Development Authority (TESDA), State Universities and Colleges (SUCs), and Local Universities and Colleges (LUCs);

(p) exercise such powers as may be necessary or incidental to the effective and efficient performance of its functions.

SECTION 44. ***Competency and Qualification Standards.*** — In coordination with the CSC and DBM, the Academy shall develop, in accordance with applicable civil service laws and rules, the competency and qualification standards of all ICT positions in the government consistent with the compensation and position classification system of the government. The Academy shall submit to the DBM its recommendation for the creation and updating of current positions for government ICT personnel; the appropriate job levels and corresponding compensation rates aligned with the personnel needs of digitally transformed government and comparable with the prevailing industry rates; and the minimum educational and professional qualification standards, duties, and functions essential to the effective operation of government ICT infrastructure and systems.

The Academy shall also define the required internationally recognized certifications and competency standards for personnel assigned or appointed to the EGov UPMO. Further, the Academy shall conduct regular trainings or coordinate and develop the required courses, multimodal training, and certifications in Project Management, Program Management, Technology Management, IT Service Management, Enterprise Architecture, Information Security, Data Privacy, and Risk Management, Data Analytics, and ICT financial planning and budgeting, among others, in support of ensuring that there are qualified individuals to fill the positions in the EGov UPMO.

SECTION 45. ***Satellite Units.*** — The Academy may establish satellite units in particular regions, provinces, or municipalities, which shall be known as Digital Transformation Centers (DTC). The Academy shall directly manage and administer the DTCs.

To ensure broader access to quality ICT training and skills development and further enhance the capability of the Academy to attain its purposes, the Academy may establish additional satellite units upon determination of the DICT.

SECTION 46. ***Establishment of Partner Satellite Units.*** — The Academy, in coordination and partnership with CHED, and TESDA, shall promulgate guidelines for the recognition and accreditation of course offerings provided by institutions under their respective purviews. Educational institutions with recognized and accredited courses shall be considered Partner Satellite Units.

The Academy and CHED shall issue guidelines on the alignment and quality of course offerings accredited by the Academy including, but not limited to, micro-credentials, short courses, ladderized pathways, credit recognition where applicable. Further, the Academy and CHED shall jointly develop an education-sector competency framework. In line with this, the Academy, in coordination with the DBM and CHED shall also issue guidelines on a fee-sharing

structure to ensure sustainability of program delivery, support capacity-building, and maintain compliance with government budgeting, accounting, and auditing rules. Fees shall be applied to courses delivered online, on site or through hybrid modalities.

The Academy shall coordinate with TESDA on the issuance of digital skills competency standards, the development of digital skills curriculum, and developing training programs for trainers and assessors in priority ICT areas.

SECTION 47. ***Accessibility.*** — The Academy shall make its services and facilities accessible to all citizens regardless of skill, age, gender, religious belief, economic status, ethnicity, physical disability, political opinion, or affiliation.

The DICT, through the Academy, shall promulgate an equitable and inclusive admission process to ensure that citizens have equal access to ICT education and that the broader base of the citizenry shall benefit from ICT education.

SECTION 48. ***Sources of Funding.*** — The Academy's operations, programs, and scholarships shall be funded from the following:

(a) allocation from DICT's budget under the annual General Appropriations Act;
(b) fees and dues collected by the Academy; and
(c) grants and donations made specifically to the Academy for its operations, in accordance with applicable laws and rules.

SECTION 49. ***Collection of Fees.*** — Based on the recommendations of the Academy, the DICT shall determine and approve the reasonable fees and necessary charges which may be collected by the Academy.

The DICT shall coordinate with the DBM and CHED for the issuance of supplemental guidelines on SUC incomes, cost-recovery schemes and training partnerships. The DICT may review and adjust the fee-sharing structure periodically based on program performance, cost requirements, and recommendations from CHED and other stakeholders.

SECTION 50. ***Donations.*** — The Academy is authorized to receive grants or donations in money, or in kind, from any source. These funds shall constitute a special trust fund administered by the DICT and shall in no case be impaired.

SECTION 51. ***Use of Funds and Donations.*** — Funds shall be retained and disbursed for the benefit of the students, faculty, trainers, consultants, and advisers, to serve the acquisition, construction, and maintenance needs of the Academy, and the proper administration of its programs.

Donations received shall be used only for the specific purposes for which they were given.

SECTION 52. ***Audit and Accountability.*** —The Academy's finances shall be administered, obligated, discharged, audited and accounted for in accordance with the procedures prescribed in relevant laws, rules, and regulations.

SECTION 53. ***Partnerships.*** — The Academy may form partnerships, collaborations, and other similar arrangements with private and public educational institutions, technical and standards organizations, and other private entities for purposes of achieving its goals and performing its functions.

Such partnerships and arrangements may include:

(a) research collaborations;

(b) resource sharing;

(c) module and training development;

(d) faculty exchange and standards development;

(e) training collaborations;

(f) internships and apprenticeships;

(g) recognition or accreditation of partner establishments and institutions and courses offered that comply with the competency standards and guidelines for government ICT workers; and

(h) other similar or relevant matters.

All partnerships entered into by the Academy shall be in accordance with the provisions of this Act and approved by the DICT Secretary. No disbursement of government funds shall be made for the purpose of establishing these partnerships.

SECTION 54. ***Course Accreditation.*** — The DICT, in coordination with TESDA and CHED, may develop guidelines for the accreditation of ICT courses offered by public and private educational institutions based on competency standards of the Academy.

RULE IX
MISCELLANEOUS PROVISIONS

SECTION 55. ***Transitory Provision.*** — The DICT, in coordination with DBM, CSC, DILG, and other relevant government agencies and instrumentalities, and in consultation with private stakeholders and civic organizations, shall study, formulate, and implement a transition master plan for the implementation of the Act and this IRR. The transition master plan shall provide for the phased adoption of the E-Government Programs, taking into account institutional readiness, existing systems, resource availability, manpower requirements, and other relevant factors, while ensuring alignment with national ICT standards and minimizing operational disruption.

The DICT shall issue the transition master plan and other guidelines for phased compliance of the Act and this IRR within ninety (90) days from effectivity of this IRR, and shall complete the transition within one (1) year from effectivity of the Act.

The creation of new positions created under the Act and this IRR shall be prioritized, subject to the review and approval of the DBM consistent with civil service laws, rules, and regulations.

SECTION 56. ***E-Government Interoperability Fund (EIF).*** — An EIF is hereby created as a special account in the general fund managed by the DICT for the implementation of E-Government Programs. The EIF may also be used for capital outlay and the maintenance and operation of ICT infrastructure, and the subscription to cloud services and other ICT systems necessary for the development, operation, maintenance, and sustainability of E-Government systems and government websites, without prejudice to the use of such funds for other purposes authorized under the Act and this IRR.

The EIF shall be sourced from donations and fees. It may also be funded through grants and loans from development and foreign partners, or through applicable Public-Private Partnership mechanisms. A portion of the Spectrum Users Fees (SUF) collected by the National Telecommunications Commission shall also accrue to the EIF.

The DICT, in coordination with the DBM, shall issue, within one hundred twenty (120) days from the effectivity of this IRR, the necessary guidelines for (i) the allocation of the SUF between the EIF and FPIAF, and (ii) collection, management, disbursement and utilization of the EIF, subject to applicable laws and existing budgeting, accounting, and auditing rules and regulations.

SECTION 57. ***Appropriations.*** — The amount necessary for the initial implementation of this Act at the national government level shall be charged against the current year's appropriations of the DICT, NTC, NPC, and other national government agencies, offices, or instrumentalities concerned. Thereafter, such sums needed for its continued implementation shall be included in the annual General Appropriations Act.

The amounts necessary to implement the Act at the local government level shall be charged against the funds of the LGU concerned.

All appropriations of the national and local government under the Act shall be subject to the existing budgeting, accounting, auditing, and other pertinent laws, rules, regulations, and guidelines.

SECTION 58. ***Applicability of Republic Act No. 8439, as Amended by Republic Act No. 11312.*** — All qualified government ICT workers involved in the planning, development, implementation and maintenance of E-Government Programs, including all DICT personnel involved in the implementation of E-Government, shall be covered by R.A. 8439, as amended by R.A. No. 11312 or the "Magna Carta for Scientists, Engineers, Researchers, and Other Science and Technology Personnel in the Government".

The DICT, in coordination with the DBM and DOST, shall issue guidelines for the implementation of this Section, including an accreditation process for eligible government workers under this Act, within ninety (90) days from effectivity of this IRR.

SECTION 59. ***Annual Reports.*** — All Covered Entities shall prepare an annual report which shall include the following:

(a) Status of the implementation of their respective E-Government initiatives based on their approved ICT Plan;

(b) Compliance by the Covered Entity with the Act and this IRR; and

(c) Performance in delivering programs and services through the E-Government to their constituencies.

Covered Entities shall submit their annual reports to the Office of the President, Senate Committee on Science and Technology or its equivalent, House of the Representatives Committee on Information and Communications Technology or its equivalent, and the DICT, and shall publish them in their respective websites and other official information portals.

SECTION 60. ***Joint Congressional Oversight Committee on E-Governance.*** — A Joint Congressional Oversight Committee on E-Governance (JCOCEG) shall be constituted to monitor and ensure the effective implementation of the Act, identify the deficiencies, limitations, and challenges in the current legal framework, and propose necessary amendments or supplementary legislation to address them.

The JCOCEG shall be composed of the following:

(a) Chairperson of the Senate Committee on Science and Technology;

(b) Chairperson of the House of Representatives Committee on Information and Communications Technology or its equivalent; and

(c) three (3) members each from the Senate and the House of Representatives. The minority in the Senate and the House of Representatives shall each have at least one (1) seat in the JCOCEG.

The Chairperson of the Senate Committee on Science and Technology and Chairperson of the House of Representatives Committee on Information and Communications Technology shall serve as co-chairpersons of the JCOCEG.

The Chairperson of the Senate Committee on Science and Technology and Chairperson of the House of Representatives Committee on Information and Communications Technology shall serve as co-chairpersons of the JCOCEG.

The JCOCEG Secretariat shall come from the existing Secretariat personnel of the Senate Committee on Science and Technology and the House of Representatives Committee on Information and Communications Technology.

The JCOCEG shall conduct a hearing at least once every quarter.

The JCOCEG shall cease to exist after five (5) years from the effectivity of the Act.

SECTION 61. ***Interpretation and Construction.*** – This IRR shall be construed and applied in accordance with, and in furtherance of, the policies and objectives of the Act.

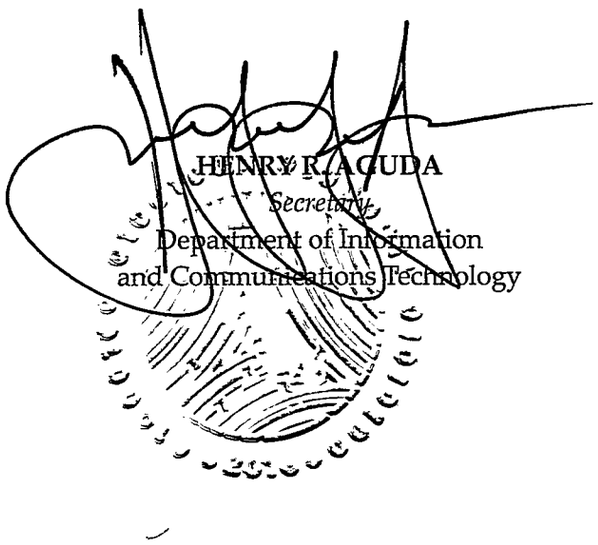
Except as may be covered by the mandate of other departments or agencies under existing laws, any conflict or ambiguity which may arise in the implementation of this IRR shall be resolved by the DICT and any requests for interpretation or opinion pertaining to this IRR should be submitted in writing to the Office of the DICT Secretary.

SECTION 62. ***Separability Clause.*** — If any provision of this IRR is held or declared unconstitutional the remainder thereof not otherwise affected shall remain in full force and effect.

SECTION 63. ***Repealing Clause.*** — All laws, presidential decrees, executive orders, letters of instruction, proclamations, or administrative regulations that are inconsistent with the provisions of the Act or this IRR are hereby repealed, amended, or modified accordingly.

SECTION 64. ***Effectivity.*** — This IRR shall take effect fifteen (15) days after its publication in the Official Gazette or in a newspaper of general circulation and upon filing of three (3) certified true copies with the Office of the National Administrative Register, University of the Philippines Law Center.

Approved:



HENRY R. AGUDA
Secretary
Department of Information
and Communications Technology