GCG *2-0707-15-11-2021-017856*

Office of the President of the Philippines
GOVERNANCE COMMISSION
FOR GOVERNMENT OWNED OR CONTROLLED CORPORATIONS
3/F, BDO Towers Paseo, 8741 Paseo De Roxas, Makati City, Philippines 1226

GOCC SECTOR ADVISORY GUIDELINES FOR CYBERSECURITY NO. 2021-01

Subject : CYBERSECURITY COMPLIANCE FOR THE GOCC SECTOR

Date : 29 October 2021

WHEREAS, on the onset of the 2019 Coronavirus Disease (COVID-19) pandemic, the public sector had faced new challenges as it adapted to an operating model in the "new normal". Government agencies and instrumentalities had accelerated their digital transformation, making cybersecurity a major concern.

WHEREAS, the risks brought about by this accelerated digital transformation could cause considerable reputational, operational, and legal implications to the public sector if neglected. Hence, in line with the State's policy, as envisioned and articulated in the National Cybersecurity Plan 2022, and recognizing the numerous threats in cyberspace, the Governance Commission had adopted the best practices in cybersecurity within its own organization to increase the security and resilience of its own data infrastructure.

WHEREAS, all the GOCCs are encouraged to do the same. In line with this, the Governance Commission is currently endeavoring to include the GOCCs compliance with cybersecurity policies and standards as a condition in the future issuance of Performance Based Bonus (PBB) guidelines.

WHEREAS, in order to prepare the GOCC Sector for the inclusion of this good governance condition in GOCC's scorecards, the Governance Commission finds it appropriate to provide GOCCs with guidance as to the necessary cybersecurity laws, issuances, and standards which it must comply with. All GOCCs are encouraged to comply with the same for the sake of improving its cybersecurity framework and critical data infrastructures.

WHEREAS, the GOCC Sector are reminded that this advisory does not exhaust all required guidelines pertaining to cybersecurity and other related matters nor should it be considered a definitive set of guidelines for purposes of compliance with the respective agencies concerned. The actual text of the various laws and issuances should still be consulted as a harmonious whole for purposes of compliance with relevant cybersecurity guidelines. The agencies tasked to implement the laws and issuances remain to be the responsible and competent entities for their respective mandates.

WHEREAS, the Governance Commission as part of its oversight functions, is fully aware that any breach of data and the cybersecurity of the GOCCs under its mandate affects the national interest of the State. Thus, the issuance of this advisory guidelines on cybersecurity.

NATIONAL CYBERSECURITY PLAN 2022

On 02 May 2017, the Department of Information and Communications Technology (DICT) officially unveiled the National Cybersecurity Plan 2022. Its goals, among others, is to develop a framework which shall institutionalize the adoption and implementation of Information Security Governance and Risk Management approaches, and other globally recognized standards to provide the government with a systematic and methodical practice of ensuring the protection of our mission critical and non-critical infostructure.[1]

The primary goals of this Plan include:

1. Making Critical Information Infrastructure (CII) Trusted and Secure;
2. Making Government Information Environment Secure;
3. Making Business Secure; and
4. Making Individuals Aware and Secure

As GOCCs are vested with functions relating to public needs which are vital to the country's socio-economic activities, any interruption of these functions and services can cause direct and significant consequences to people's safety and security. Thus, GOCCs are encouraged to align their cybersecurity framework to the cybersecurity policy direction of the Philippine Government as laid down in its National Cybersecurity Plan 2022.

For a detailed discussion on the National Cybersecurity Plan 2022, you may visit https://dict.gov.ph/national-cybersecurity-plan-2022.

NATIONAL SECURITY POLICY 2017-2022

Executive Order No. 16 (s. 2017)[2] mandated all government departments and agencies, including GOCCs, to adopt the National Security Plan (NSP) 2017-2022 in the formulation and implementation of all their plans and programs which have national security implications.[3]

The NSP is a document which provides a roadmap for the attainment of the Government's national security vision and aspirations within six years, as well as prescribes the courses of action that it would undertake to achieve the purpose.

Among the issues and challenges recognized by the NSP is the rising threat of cybercrime in the Philippines. The NSP discussed that the country must develop its cyber capabilities to address the evolving security challenges in cyberspace. Among its directives is to enhance and expand its pool of information communication technology (ICT) experts to equip the government with the necessary skills to preempt and combat cyber-based crimes.[4]

To conform with the policy directives of the national government in its NSP, GOCCs should endeavor to prioritize collaboration with the academe and the business

[1] National Cybersecurity Plan 2022, Executive Summary
[2] Directing All Government Department and Agencies, Including Government-Owned or -Controlled Corporations and Local Government Units to Adopt the National Security Policy 2017-2022 in the Formulation and Implementation of their National Security Related Plans and Programs
[3] Section 1, E.O. No. 16 (s. 2017)
[4] Page 17, National Security Plan 2017-2022

community for cybersecurity trainings and certifications of members of its information technology units to build or improve their capabilities against cybercrimes. Likewise, GOCCs should equip its information technology professionals with the appropriate infrastructure for it to properly address the challenges brought about the rise of cybercrimes.

DATA PRIVACY ACT OF 2012

In 2012, Republic Act No. 10173[5] or otherwise known as the "Data Privacy Act of 2012" was passed into law. The said law was passed *"to protect the fundamental human right to privacy of communication while ensuring free flow of information to promote innovation and growth [and] the [State's] inherent obligation to ensure that personal information in information and communications systems in government and in the private sector are secured and protected".*[6]

Through this law, the National Privacy Commission (NPC) was created to administer its implementation. It was likewise tasked to monitor and ensure compliance of the private and public sector with R.A. No. 10173 and international standards for personal data protection.

To comply with the Data Privacy Act of 2012, GOCCs must conform with the five (5) pillars of compliance as required by the said law:

1. Appoint a Data Protection Officer (DPO)[7]

Appointment of a Data Protection Officer (DPO) is a legal requirement for Personal Information Controllers (PICs) and Personal Information Processors (PIPs), under the Data Privacy Act of 2012. The DPO shall be in charge with the organization's compliance with the Data Privacy Act of 2012, its IRR, issuances by the NPC, and other data protection standards.

GOCCs should endeavor the designation of a DPO for it to ensure the protection of the personal data, not only of its employees, but external stakeholders as well. This shall not only make a GOCC competitive in the landscape of data protection, but also improve its service to the public.

For a detailed and step-by-step guideline on the DPO registration process, please visit https://www.privacy.gov.ph/guidelines-on-dpo-registration-process/

2. Conduct a Privacy Impact Assessment (PIA)[8]

A PIA is an instrument for assessing the potential impacts on privacy of a process, information system, program, software module, device or other initiative which processes personal information and in consultation with stakeholders, for taking actions as necessary to treat a privacy risk.[9]

[5] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes
[6] Section 2, R.A. No. 10173
[7] Section 21, R.A. No. 10176, NPC Circular No. 16-01, NPC Advisory 17-01
[8] Section 20(c), R.A. No. 10176, Section 29 of the IRR, NPC Advisory No. 17-03
[9] Chapter II, National Privacy Commission Toolkit

The NPC does not provide for the specific methodology or frequency of conducting a PIA. When conducting a PIA, GOCCs are at liberty to formulate its own PIA process that caters to its concerns and needs taking into consideration its operations and size of the organization.

3. Creation of a Privacy Management Program (PMP)[10]

A PMP is described by the NPC as a holistic approach to privacy and data protection which minimizes the risks of privacy breaches, maximizes the ability to address underlying problems, and reduce the damage arising from breaches.[11]

Through the PMP, an organization's commitment to building trust with its stakeholders is shown as it becomes transparent to its privacy policies and practices.

GOCCs should adopt its own PMP to show its stakeholders its commitment to embed privacy and data protection in its strategic framework and daily operations. Furthermore, adoption of a PMP shall coordinate the GOCC's data protection projects and activities, hence, allowing the efficient use of its available resources.

4. Implementation of Privacy and Data Protection Measures[12]

Under this requirement, a GOCC should develop and document internal policies that address its obligations under the Data Privacy Act of 2012 through the crafting and implementation of a Privacy Manual. A Privacy Manual encapsulates all data privacy and protection protocols that need to be observed and carried out within the organization.

Aside from having a Privacy Manual, a GOCC should likewise incorporate in its daily operations a Privacy Notice and Privacy Policy. These are statements made to a data subject that describes how the organization collects, uses, retains, and discloses personal information. It aims to give its stakeholders the opportunity to be apprised of what, how and why personal data is being collected from them.

5. Maintaining a Breach Reporting Procedure[13]

GOCCs should likewise have a clearly defined and up-to-date standard procedure in place for the handling, investigation and reporting of data privacy security incidents. Furthermore, a Security Incident Response Team which shall ensure the timely action in the event of a security incident or personal data breach should be constituted.

This team, to be prepared to handle data privacy breaches, should be knowledgeable of breach reporting requirements of the Data Privacy Act of 2012 and other issuances of the NPC, supplemented by sufficient trainings

[10] Sections 11-15, R.A. No. 10176, Section 21-23 ad 43-45 of the IRR, NPC Circular 16-01 and 16-02
[11] Chapter II, NPC Privacy Toolkit
[12] Sections 16-18 and 38 of R.A. No. 10176, Sections 17-24, 34-37 of the IRR, and NPC Circular No. 16-04
[13] Sections 20.f and 30 of R.A. No. 10176, Sections 38-42 ad 57 of the IRR, NPC Circular No. 16-03

on breach response. Breach response drills should likewise be performed at least once a year to immerse this team in handling security incidents.

Aside from compliance with the foregoing, GOCCs are encouraged to register with the NPC its data processing systems and if applicable to the GOCC's operations, notify it with its automated processing operations.

NPC Circular No. 17-01[14] requires organizations to register its data processing systems if it is processing personal data and operating in the country under the following conditions:[15]

a. An individual or institution employs at least 250 employees.
b. The processing involves sensitive personal information of at least 1,000 individuals.
c. The processing likely to pose a risk to the rights and freedoms of data subjects; or
d. The processing is not occasional

Furthermore, where the processing of personal data becomes the sole basis of making decisions about a data subject and when the decisions would significantly affect the data subject (profiling based on an individual's economic situation, political or religious beliefs, behavioral or marketing activities, electronic communication data, location data and financial data), the GOCC should notify the NPC via its mandatory registration process.[16]

GOCCs are encouraged to keep itself updated on the registration processes and notification requirements laid down by the NPC.

CYBERCRIME PREVENTION ACT OF 2012

R.A. No. 10175 or otherwise known as the "Cybercrime Prevention Act of 2012" was enacted to address legal issues concerning online interactions and the internet in the Philippines. This landmark legislation criminalized several types of offenses including illegal access (hacking), data interference, device misuse, cybersquatting, computer-related offenses such as computer fraud, content-related offenses such as cybersex and spam, and other offenses.

Aside from identifying the above-mentioned punishable acts, the law likewise laid down the government entities involved in the enforcement, implementation, and administration of this law. Among these entities are as follows:

I. **Department of Justice (DOJ)**;

In line with the mandates under R.A. No. 10175 and its IRR, the DOJ-Office of Cybercrime (OOC) was created to act as the central authority in all matters related to international mutual assistance and extradition. Section 28 of the IRR provides for the specific functions and duties of the DOJ-OOC, to wit:

[14] Registration of Data Processing and Notifications regarding Automated Decision-Making
[15] Section 5, NPC Circular No. 17-01
[16] Section 24, NPC Circular No. 17-01

"Section 28. *Department of Justice (DOJ); Functions and Duties.* – The DOJ-Office of Cybercrime (OOC), designated as the central authority in all matters related to international mutual assistance and extradition, and the Cybercrime Operations Center of the CICC, shall have the following functions and duties:

a. Act as a competent authority for all requests for assistance for investigation or proceedings concerning cybercrimes, facilitate the provisions of legal or technical advice, preservation and production of data, collection of evidence, giving legal information and location of suspects;
b. Act on complaints/referrals, and cause the investigation and prosecution of cybercrimes and other violations of the Act;
c. Issue preservation orders addressed to service providers;
d. Administer oaths, issue subpoena and summon witnesses to appear in an investigation or proceedings for cybercrime;
e. Require the submission of timely and regular reports including pre-operation, post-operation and investigation results, and such other documents from the PNP and NBI for monitoring and review;
f. Monitor the compliance of the service providers with the provisions of Chapter IV of the Act, and Rules 7 and 8 hereof;
g. Facilitate international cooperation with other law enforcement agencies on intelligence, investigations, training and capacity-building related to cybercrime prevention, suppression and prosecution;
h. Issue and promulgate guidelines, advisories, and procedures in all matters related to cybercrime investigation, forensic evidence recovery, and forensic data analysis consistent with industry standard practices;
i. Prescribe forms and templates, including, but not limited to, those for preservation orders, chain of custody, consent to search, consent to assume account/online identity, and request for computer forensic examination;
j. Undertake the specific roles and responsibilities of the DOJ related to cybercrime under the Implementing Rules and Regulation of Republic Act No. 9775 or the "Anti-Child Pornography Act of 2009"; and
k. Perform such other acts necessary for the implementation of the Act."

II. **National Bureau of Investigation (NBI)**;
III. **Philippine National Police (PNP);** and

These law enforcement authorities are responsible of the efficient and effective law enforcement of the provisions of R.A. No. 10175.[17] For this purpose, special cybercrime divisions and units were formed by these law enforcement authorities with the following powers and functions:

"*Section 10. Powers and Functions of Law Enforcement Authorities. – The NBI and PNP cybercrime unit or division shall have the following powers and functions:*

a. Investigate all cybercrimes where computer systems are involved;
b. Conduct data recovery and forensic analysis on computer systems and other electronic evidence seized;

[17] Section 9, Implementing Rules and Regulations of the Cybercrime Prevention Act

c. *Formulate guidelines in investigation, forensic evidence recovery, and forensic data analysis consistent with industry standard practices;*
d. *Provide technological support to investigating units within the PNP and NBI including the search, seizure, evidence preservation and forensic recovery of data from crime scenes and systems used in crimes, and provide testimonies;*
e. *Develop public, private sector, and law enforcement agency relations in addressing cybercrimes;*
f. *Maintain necessary and relevant databases for statistical and/or monitoring purposes;*
g. *Develop capacity within their organizations in order to perform such duties necessary for the enforcement of the Act;*
h. *Support the formulation and enforcement of the national cybersecurity plan; and*
i. *Perform other functions as may be required by the Act."*

IV. **Cybercrime Investigation and Coordinating Center (CICC)**

The CICC is an inter-agency body created under R.A. No. 10175 mandated with the policy coordination among concerned agencies and for the formulation and enforcement of the National Cyber Security Plan.

According to Section 27 of the IRR of R.A. No. 10175, the CICC shall have the following powers and functions:

a. *"Formulate a national cybersecurity plan and extend immediate assistance for the suppression of real-time commission of cybercrime offenses through a computer emergency response team (CERT);*
b. *Coordinate the preparation of appropriate and effective measures to prevent and suppress cybercrime activities as provided for in the Act;*
c. *Monitor cybercrime cases being handled by participating law enforcement and prosecution agencies;*
d. *Facilitate international cooperation on intelligence, investigations, training and capacity-building related to cybercrime prevention, suppression and prosecution through the DOJ-Office of Cybercrime;*
e. *Coordinate the support and participation of the business sector, local government units and NGOs in cybercrime prevention programs and other related projects;*
f. *Recommend the enactment of appropriate laws, issuances, measures and policies;*
g. *Call upon any government agency to render assistance in the accomplishment of the CICC's mandated tasks and functions;*
h. *Establish and perform community awareness program on cybercrime prevention in coordination with law enforcement authorities and stakeholders; and*
i. *Perform all other matters related to cybercrime prevention and suppression, including capacity-building and such other functions and duties as may be necessary for the proper implementation of the Act."*

It is likewise worth noting that Section 26 of the IRR also mandates the CICC to enlist the assistance of any other agency of the government **including government owned and -controlled corporation** in the performance of its functions.

GOCCs are encouraged to align its cybersecurity policies with those issued by the above-mentioned authorities and to ensure full cooperation with these authorities

when the need arises. Furthermore, GOCCs are likewise encouraged to integrate the recognition and prevention of the punishable acts under R.A. No. 10175 and its Implementing Rules and Regulations into its respective frameworks.

ACCESS DEVICE REGULATION ACT OF 1998

Republic Act No. 8484 of otherwise known as the *"Access Devices Regulation Act of 1998"* regulates the issuance and use of access devices punishes fraudulent acts committed relative thereto.

The cybersecurity policy laid down in this law, specifically on reporting requirements, are applicable to GOCCs engaged in the banking and finance business which issues and/or uses access devices.

GOCCs engaged in banking and finance are encouraged to comply with Section 16 of R.A. No. 8484, to wit:

> *"Section 16. Reporting requirements. – All companies engaged in the business of issuing access devices, including banks, financing companies and other financial institutions issuing access devices, shall furnish annually, on or before the 31st of March of the succeeding year, a report to the Credit Card Association of the Philippines regarding access device frauds committed against the holders of such entities in the preceding calendar year, for consolidation and submission to the National Bureau of Investigation. Notwithstanding this requirement, banks, financing companies and other financial institutions, including their subsidiaries and affiliates, issuing access devices shall continue to be regulated and supervised by the Bangko Sentral ng Pilipinas while other companies issuing access devices shall continue to be regulated and supervised by the Securities and Exchange Commission."*

MEMORANDUM ORDER NO. 37 (S. 2001)

In 2001, Former President Gloria Macapagal-Arroyo issued M.O. No. 37 entitled *"Providing for the Fourteen Pillars of Policy and Action of the Government Against Terrorism"*. This issuance was anchored on the Philippines' intention to implement the United Nations Security Council Resolution No. 1368 as a charter member of the United Nation's Coalition Against Terrorism.

Items Nos. 4 and 10 of Article III of the issuance provides for certain compliance and audit requirements which covers GOCCs. The said items provide that:

> *"Article III, No. 4: <u>Accountability of public and private corporations and personalities.</u>*
>
> *The DILG and the SEC shall conduct an inventory of all public or private corporations and personalities reasonably suspected of working as fronts of terrorists or of involvement in terrorist activities or in aiding and abetting terrorists. Information obtained by the DILG and the SEC shall be made available to the relevant government agencies. The DILG and the SEC shall institute all necessary legal proceedings to suppress the activities of such public and private corporations and personalities."*

Article III, No. 10: Comprehensive Security Plans for Critical Infrastructure.

In coordination with other responsible departments and agencies of the government and with the private sector, the Cabinet Oversight Committee shall prepare a comprehensive security plan for critical infrastructure which shall include, without limitation, power plants, power transmission and distribution facilities, oil and gas depots, key public works structures, vital communications installations, public and private buildings and other facilities in the center of commerce and industry."

These requirements are intended to involve both private and public corporations in the Philippine Government's goal of suppressing terrorist acts and making those responsible for aiding, supporting, or harboring the perpetrators, organizers, and sponsors of these act as accountable. GOCCs are encouraged to align their policies with M.O. No. 37 (s. 2001) and coordinate with the above-mentioned government agencies for the fulfillment of the requirements under this law.

ELECTRONIC COMMERCE ACT OF 2000

In line with the policies under Republic Act No. 8792 or otherwise known as the *"Electronic Commerce Act of 2000"* aimed to the recognition of the validity and binding effect of data messages, electronic documents, and electronic signatures, GOCCs must be able to authenticate their issuances legally. For example, key signatory officials shall secure their digital signatures by registering with the DICT through the Philippine National Public Key Infrastructure (PNPKI).

Guidelines for the PNPKI may be accessed through this link: Philippine National Public Key Infrastructure (PNPKI) | DICT

ANTI-PHOTO AND VIDEO VOYEURISM ACT OF 2009

GOCCs are likewise reminded to integrate into their cybersecurity policies the recognition and prevention of the prohibited acts penalized under Republic Act No. 9995 or otherwise known as the *"Anti-Photo and Video Voyeurism Act of 2009".*

The following are the prohibited acts under the said law:

"Section 4. Prohibited Acts. - It is hereby prohibited and declared unlawful for any person:

(a) To take photo or video coverage of a person or group of persons performing sexual act or any similar activity or to capture an image of the private area of a person/s such as the naked or undergarment clad genitals, pubic area, buttocks or female breast without the consent of the person/s involved and under circumstances in which the person/s has/have a reasonable expectation of privacy;

(b) To copy or reproduce, or to cause to be copied or reproduced, such photo or video or recording of sexual act or any similar activity with or without consideration;

(c) To sell or distribute, or cause to be sold or distributed, such photo or video or recording of sexual act, whether it be the original copy or reproduction thereof; or

(d) To publish or broadcast, or cause to be published or broadcast, whether in print or broadcast media, or show or exhibit the photo or video coverage or recordings of such sexual act or any similar activity through VCD/DVD, internet, cellular phones and other similar means or device.

The prohibition under paragraphs (b), (c) and (d) shall apply notwithstanding that consent to record or take photo or video coverage of the same was given by such person/s. Any person who violates this provision shall be liable for photo or video voyeurism as defined herein.

Section 5. Penalties. - The penalty of imprisonment of not less that three (3) years but not more than seven (7) years and a fine of not less than One hundred thousand pesos (P100,000.00) but not more than Five hundred thousand pesos (P500,000.00), or both, at the discretion of the court shall be imposed upon any person found guilty of violating Section 4 of this Act."

If the violator is a juridical person, its license or franchise shall automatically be deemed revoked and the persons liable shall be the officers thereof including the editor and reporter in the case of print media, and the station manager, editor and broadcaster in the case of a broadcast media.

If the offender is a public officer or employee, or a professional, he/she shall be administratively liable.

If the offender is an alien, he/she shall be subject to deportation proceedings after serving his/her sentence and payment of fines."

ANTI-CHILD PORNOGRAPHY ACT OF 2009

In addition to the prohibited acts under Republic Act No. 9995, GOCCs are likewise encouraged to integrate into their cybersecurity policies the recognition of the prohibited acts penalized under Republic Act No. 9775 or otherwise known as the *"Anti-Child Pornography Act of 2009"*

The following are the prohibited acts under the said law:

"Section 4. Unlawful or Prohibited Acts. - It shall be unlawful for any person: (a) To hire, employ, use, persuade, induce or coerce a child to perform in the creation or production of any form of child pornography; (b) To produce, direct, manufacture or create any form of child pornography; (c) To publish offer, transmit, sell, distribute, broadcast, advertise, promote, export or import any form of child pornography; (d) To possess any form of child pornography with the intent to sell, distribute, publish, or broadcast: Provided. That possession of three (3) or more articles of child pornography of the same form shall be prima facie evidence of the intent to sell, distribute, publish or broadcast; (e) To knowingly, willfully and intentionally provide a venue for the commission of prohibited acts as, but not limited to, dens, private rooms, cubicles, cinemas, houses or in establishments purporting to be a legitimate business; (f) For film distributors, theaters and

telecommunication companies, by themselves or in cooperation with other entities, to distribute any form of child pornography; (g) For a parent, legal guardian or person having custody or control of a child to knowingly permit the child to engage, participate or assist in any form of child pornography; (h) To engage in the luring or grooming of a child; (i) To engage in pandering of any form of child pornography; (j) To willfully access any form of child pornography; (k) To conspire to commit any of the prohibited acts stated in this section. Conspiracy to commit any form of child pornography shall be committed when two (2) or more persons come to an agreement concerning the commission of any of the said prohibited acts and decide to commit it; and (l) To possess any form of child pornography.

Section 11. Duties of an Internet Content Host. - An internet content host shall: (a) Not host any form of child pornography on its internet address; (b) Within seven (7) days, report the presence of any form of child pornography, as well as the particulars of the person maintaining, hosting, distributing or in any manner contributing to such internet address, to the proper authorities; and (c) Preserve such evidence for purposes of investigation and prosecution by relevant authorities."

Section 11 of the law must be considered especially in the websites of the GOCCs.

Relative to both R.A. No. 9775 and R.A. No. 9995, GOCCs must ensure that the internet access in their offices is properly monitored to prevent the exchange of contraband digital assets defined in the statutes.

DICT CIRCULAR NOS. 2017-001 & 2020- 06

Pursuant to the provisions of the Electronic Commerce Act of 2000, its Implementing Rules and Regulations, and the Executive Order (EO) No. 810 issued on 15 June 2009[18], government agencies and instrumentalities providing electronic services to its clients are required to use digital signatures in their respective e-government services to ensure confidentiality, authenticity, integrity, and non-repudiation of electronic transactions in government.

The DICT Circular NO. 2017 – 001[19] provided the guidelines on the application and issuance of Philippine National Public Key Infrastructure (PNPKI) digital certificates. Government agencies, GOCCs, and personnel, private individuals, government computers, servers, and machines are encouraged to avail the Public Key Infrastructure (PKI) being offered by the DICT. The PKI allows users of public networks like the Internet to exchange private data securely.

During the declared state of public health emergency due to the Coronavirus Disease 2019 (COVID-19) situation, the procedures for the processing of application for the issuance of PNPKI digital certificates set under DICT Circular 2020-006[20] shall be followed. After the state of public health emergency has been lifted, the previously prescribed rules under DICT Circular 2017-001 shall strictly be followed.

[18] Institutionalizing the Certification Scheme for Digital Signatures and Directing the Application of Digital Signatures in E-Government Services
[19] Amending the Philippine National Public Key Infrastructure (PNPKI) Root Certification Authority Certificate Policy Version 1.0
[20] Guidelines on the Application and Issuance of PNPKI Digital Certificates for External Clients During the State of Public Health Emergency.

For further inquiries and submission of application requirements, please email **info.pnpki@dict.gov.ph** or the PNPKI Cluster Team Offices (https://dict.gov.ph/pnpki-where-to-submit/) in the Region.

GOVERNMENT WEB HOSTING SERVICE

The Integrated Government Philippines (iGovPhil) Program provides a web hosting service to government entities, including government agencies, financial institutions, government-owned and -controlled corporations, and inter-agency collaborations, programs, and projects. This allows government websites to be housed under one roof.

Pursuant to Administrative Order No. 39, s. 2013, government agencies are mandated to transfer their Internet hosting requirements to the **Government Web Hosting Service (GWHS)** for more efficient use of technology and greater protection against hacking and cyber-attacks. All government agencies including GOCCs are also tasked to strictly follow the **Uniform Website Content Policy (UWCP)** that gives their websites a common look and feel and the government a corporate identity.

The DICT's GWHS provides the following services to government agencies including GOCCs:

a. Web Hosting Service ONLY
b. Domain Name System (DNS) Hosting Service ONLY
c. DNS Hosting and Web Hosting Service
d. .gov.ph DNS Registration, DNS Hosting, and Web Hosting Service
e. Updating of GWHS account information

The details and the complete requirements for the application on the aforesaid services can be found through the link: https://dict.gov.ph/gwhs/

DICT CIRCULAR NO. 2017-005

Pursuant to the National Cybersecurity Plan (NCSP) 2022, government agencies including GOCCs are reminded to adopt the policies, rules, and regulations on the protection of Critical Infostructure (CII).

To achieve the objectives of the NCSP 2022, organizations are expected to implement the PNS ISO/IEC 27000 Family of Standards and other relevant International Standards by all Critical Information Infrastructure or Critical Infostructure (CII) operators. According to the Circular, CII refers to *the computer system, and/or networks whether physical or virtual, and/or computer programs, computers data and/or traffic data that vital to the country that the incapacity or destruction of 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 mattes. Sectors initially classified as CIIs are the following: government, transportation (land, sea, air), energy, water, health, emergency services, banking and finance, business process outsourcing, telecommunications, media.* Sectors not classified as CII shall adopt the PNS ISO/IEC 27002 on voluntary basis.

Other relevant policies, rules, and regulations on the protection of CII stipulated in the Circular are the requirement for CII operators to:

a. participate in the conduct of risk and vulnerability assessment;
b. participate in the conduct of a security assessment program of the DICT;
c. create their own Computer Emergency Response Team (CERT);
d. obtain a Cybersecurity Compliance Certificate issued by the DICT;
e. for telecommunication operators and ISPs to conduct Cyber Hygiene activities;
f. obtain the Seal of Cybersecurity (SCS) upon compliance to the prescribed requirements;
g. development and implementation of Disaster Recovery Plan (DR Plan) and Business Continuity Plan (BCP) as part of the ICT programs;
h. participate in the conduct of national cyber drills by the DICT;
i. comply with the issuances from the National Privacy Commission;
j. to be subjected to a monitoring and evaluation system to be established by DICT; and
k. creation of a Sectoral CERT.

DICT CIRCULAR NO. 2017-002 & 2020-010

Pursuant to the Section 2(b) of Republic Act No. 10844[21] the DICT issued the Department Circular No. 2017-002 prescribing the policy of the government to adopt a "cloud first" approach and for government departments and agencies including GOCCs to consider cloud computing solutions as a primary part of their infostructure planning and procurement.

Section 5 of the Circular states that:

> *"5.2 All government agencies shall adopt cloud computing as the preferred ICT deployment strategy for their own administrative use and delivery of government online services, except:*
>
> *5.2.1 When it can be shown that an alternative ICT deployment strategy meets special requirements of a government agency; and*
>
> *5.2.2 When it can be shown that an alternative ICT deployment strategy is more cost effective from a Total Cost of Ownership (TCO) perspective and demonstrates at least the same level of security assurance that a cloud computing deployment offers."*

Due to the "new normal" amidst the Coronavirus Disease 2019 (COVID-19) pandemic, the DICT recently amended its Cloud First Policy through **DICT CIRCULAR NO. 2020-010** to provide clearer instructions on policy coverage, data classification, and data security, as well as its policy on sovereignty, residency, and ownership.

[21] Declared as a policy of the state to ensure the provision of a strategic, reliable, cost-efficient and citizen-centric information and communications technology infrastructure (infostructure), systems and resources as instruments of good governance and global competitiveness

As amended, the Cloud First Policy covers all departments, bureaus, offices, and agencies of the Executive Branch, Government Owned and/or Controlled Corporations (GOCCs), State Universities and Colleges (SUCs), Local Government Units (LGUs), and all cloud service providers and private entities rendering services to the government. Moreover, the Congress, the Judiciary, the Independent Constitutional Commissions, and the Office of the Ombudsman are also encouraged to adopt the Cloud First Policy.

To avail the GovCloud service being offered by the Integrated Government Philippines Program of the DICT & DOST – ASTI, you may refer to this link: https://i.gov.ph/govcloud/avail/

INTERNATIONAL STANDARDS FOR INFORMATION SECURITY AND CYBERSECURITY

GOCCs are encouraged to obtain certifications or adopt guidance from existing international industry standards and best practices to help organizations manage their cybersecurity risks. The following are some of the Information Security and Cybersecurity standards and frameworks that GOCCs use:

a. **ISO 27000 Family or Information Security Management Systems (ISMS)**. A systematic approach to managing sensitive company information that ensures its security. It includes people, processes, and IT systems by applying a risk management process. It can help businesses of any size keep their information assets secure.

b. **ISO/IEC 27001:2013.** Applicable mainly to organizations that maintain data centers, this specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of an organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of an organization. The requirements set out are generic and are intended to be applicable to all organizations, regardless of type, size, or nature.

c. **ISO/IEC 27032 –** It provides guidance on addressing a wide range of cybersecurity risks, including user endpoint security, network security, and critical infrastructure protection.

d. **ISO/IEC 27018:2014.** This establishes commonly accepted control objectives, controls, and guidelines for implementing measures to protect personal information in accordance with the privacy principles in ISO/IEC 29100, which, in turn, concerns public cloud computing environments. It also specifies guidelines based on ISO/IEC 27002, considering the regulatory requirements for the protection of personal information that might be applicable within the context of the information security risk environment(s) of a (public) cloud service provider. It may be used by organizations of any type and size, including public and private companies, government entities, and non-profit organizations, which provide information processing services as Personal Information Processors (PIP) via cloud computing under contract to other organizations.

e. **NIST Cybersecurity Framework-** This cybersecurity framework provides a set of guidelines and best practices to help organizations build and improve cybersecurity posture. The framework puts forth a set of recommendations and standards that enable organizations to be better prepared in identifying and detecting cyber-attacks, and provides guidelines on how to respond, prevent, and recover from cyber incidents

f. **Service Organization Control (SOC) Type 2 -** This is a trust-based cybersecurity framework and auditing standard developed by the American Institute of Certified Public Accountants (AICPA) to help verify that vendors and partners are securely managing client data.

g. **NERC-CIP-** This is a set of cybersecurity standards designed to help those in the utility and power sector reduce cyber risk and ensure the reliability of bulk electric systems.

h. **HIPAA –** This is a cybersecurity framework that requires healthcare organizations to implement controls for securing and protecting the privacy of electronic health information. In addition to demonstrating compliance against cyber best practices such as training employees, companies must also conduct risk assessments to manage and identify emerging risk.

i. **Recommendation ITU-T X.1205 -** This provides a definition for cybersecurity and taxonomy of the security threats and vulnerabilities from an organization point of view including the most common hacker's tools of the trade are presented. Threats are also discussed at various network layers and various cybersecurity technologies that are available to remedy the threats including: routers, firewalls, antivirus protection, intrusion detection systems, intrusion protection systems, secure computing and audit and monitoring. Further, risk management strategies and techniques are discussed in the Recommendation including the value of training and education in protecting the network.

j. Furthermore, GOCCs may also adopt other standards that may be applicable to the operation and needs of an organization.

FUTURE POLICY INSTRUCTION

Although the Governance Commission recognizes that it is not a competent authority when it comes to cybersecurity, information security and data privacy, it may, as the central advisory, monitoring, and oversight body of GOCCs, endeavor to include the GOCCs compliance with cybersecurity policies and standards enforced by competent authorities as a subject/condition of future issuance of PBB guidelines.

These requirements will not only encourage GOCCs to comply with relevant laws, rules, and standards on cybersecurity, but also protect the interest of the public in this ever-changing digital era.

On a final note, the thrust of the Governance Commission in issuing this advisory guidelines for cybersecurity is for the GOCCs' substantial compliance of the various laws, rules, procedures and regulations relating to cybersecurity and data

privacy. Thus, the GOCC Sector is strongly encouraged to align their policies to the directives of the competent authorities on cybersecurity and data privacy, and create or improve its respective cybersecurity framework, enterprise risk assessment, regular penetration testing and adoption of a manual on data privacy.

FOR THE GUIDANCE OF THE GOCC SECTOR.