REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

DEPARTMENT CIRCULAR NO. 007 APR 16 2020
Series of 2020

FOR : **ALL MANAGEMENT INFORMATION SYSTEM (MIS) OFFICERS AND SERVER ADMINISTRATORS**
National Government Departments, Bureaus, Offices, Agencies, State Universities and Colleges, Government-Owned or Controlled Corporations, Local Government Units, Government Instrumentalities, Constitutional Commissions, Congress of the Philippines, the Philippine Judiciary, Office of the Ombudsman.

RE : **PRESCRIBING THE USE OF UPDATED VERSIONS OF CRYPTOGRAPHIC PROTOCOLS FOR ALL GOVERNMENT OWNED, CONTROLLED, MANAGED, CONTRACTED, OR SPONSORED WEBSITES.**

WHEREAS, it is the declared policy of the State to: (1) ensure universal access to quality, affordable, reliable, and secure Information and Communications Technology (ICT) services;[1] (2) promote the development and widespread use of emerging ICT, and to foster and accelerate the convergence of ICT facilities;[2] (3) ensure the rights of individuals to privacy and confidentiality of their personal information;[3] and (4) ensure the security of critical ICT infrastructures including information assets of the government, individuals, and businesses;[4]

WHEREAS, under Republic Act (RA) No. 8792, otherwise known as the "*Electronic Commerce Act of 2000*," it is the declared policy of the state to: (1) facilitate the transfer and promotion of technology; (2) ensure network security, connectivity and neutrality of technology for the national benefit; and (3) marshal, organize and deploy national information infrastructures, comprising in both telecommunications network and strategic information services, including their interconnection to the global information networks, with the necessary and appropriate legal, financial, diplomatic and technical framework, systems and facilities;

WHEREAS, Executive Order (EO) No. 810, series of 2009, otherwise known as *"Institutionalizing the Certification Scheme for Digital Signatures and Directing the Application of Digital Signatures in E-Government Services"*, provided the guidelines on the application of digital signature in the government and private sector;

WHEREAS, in compliance with §3(a), EO No. 810 s. 2009, the Department of Information and Communications Technology (DICT) issued Department Circular (DC) No. 2017-001, amending the Philippine National Public Key Infrastructure (PNPKI) Certificate

[1] §2(c), Republic Act (RA) No. 10844.
[2] §2(d), RA 10844.
[3] §2(l), RA 10844.
[4] §2(m), RA 10844.

D.I.C.T.
RECORDS SECTION
CERTIFIED COPY
ADELINA A. OBLIGACION
Administrative Officer IV
5/13/2020

DICT Building, C.P. Garcia Avenue Diliman, Quezon City 1101, Philippines
+632 8920 0101 | www.dict.gov.ph

Policy (CP) version 1.0, in operating the Philippine Root Certification Authority (RootCA) and Government Certification Authority (GovCA);

WHEREAS, DC No. 2017-001, in implementing the PNPKI CP version 2.0, provided the guidelines on the application and issuance of PNPKI digital signature certificates to DICT officials, personnel, and external clients in the delivery of e-government services to ensure confidentiality, authenticity, integrity, and non-repudiation of electronic transactions in the government;

WHEREAS, cybersecurity threats have become a serious concern on a global scale, thus, placing all types and sizes of user data at risk;

WHEREAS, pursuant to the Philippine National Cybersecurity Plan (NCSP), it is in the public interest that government ICT systems be secured to ensure the protection of information systems (hardware and software including associated and support infrastructure), the written or electronic data and other vital information of both sender and end-user within these systems, and the services that are provided by these systems, are encrypted and protected from unauthorized access, harm or misuse, whether intentional or accidental;[5]

WHEREAS, the data and information within the ICT network systems are critical assets that must be protected and secured from being compromised or breached;[6]

WHEREAS, the Philippine NCSP strategic objectives focus on technical, administrative, and procedural measures to promote the adoption of cybersecurity measures among individuals, and to enhance the security and resilience of critical information infrastructure and its component government, public and military networks, in order to deal with sophisticated cyber attacks;[7]

WHEREAS, with government agencies being the first line of defense in the protection of critical information infrastructure, the Philippine NCSP aims to institutionalize information security across all government agencies, and mandates them to implement policies and procedures to cost-effectively reduce risks to acceptable levels;[8]

WHEREAS, Information Technology (IT) due diligence and best practices include the use and constant updating of cryptographic protocols for secure connections to ensure a safer experience for end users, achieve a stronger search engine optimization ranking, and stable encryption of sensitive data;

WHEREAS, Transport Layer Security (TLS) in its current version is the cryptographic protocol and Internet Engineering Task Force (IETF) Standard widely used to provide end-to-

[5] DICT National Cybersecurity Plan 2022, p.8.
[6] Id. at p.11.
[7] Id. at p. 17.
[8] Id at. 25.

D.I.C.T.
RECORDS SECTION
CERTIFIED COPY
ARLENA A. CALIGACION
Administrative Officer IV
5/13/2022

end communications security for internet communications and online transactions in order to prevent network eavesdropping, data tampering, and message/information forgery;[9]

NOW, THEREFORE, in view of the foregoing, in the exigency of public service and pursuant to the afore-mentioned issuances of the Philippine Government, as well as the provisions of existing laws, rules and regulations, this Circular is hereby issued:

Section 1. Adoption, Use, and Implementation of Current Version of TLS Protocol in the Government.—Pursuant to the National Cybersecurity Plan, the provisions of existing laws, rules and regulations, and for purposes of ensuring communications security over the network to protect the public interest, the adoption, utilization, and implementation of the Transport Layer Security (TLS) Protocol in its updated version is hereby prescribed for all the departments, bureaus, offices, and other agencies of the national government, state universities and colleges, government-owned or controlled corporations, local government units, and other government instrumentalities, including the Constitutional Commissions, Congress, the Judiciary, Office of the Ombudsman.

Section 2. Duty of the MIS Officer and Server Administrators; TLS Certificate.— The management information system (MIS) officer and server administrator shall be primarily responsible for the procurement and/or continuing use of the updated version of the TLS protocol for all the websites owned, controlled, managed, contracted, or sponsored by their respective government agencies or instrumentalities. For websites owned or managed by private individuals or entities with existing contracts with any of the government agencies or instrumentalities, the responsibility shall be shared jointly and severally with the individual or entity so contracted.

The MIS officer and/or server administrator shall have all their existing web servers configured and/or migrated to the updated version of the TLS protocol,[10] and duly supported by appropriate TLS certificates issued by duly-recognized Certificate Authority Organizations.[11]

Any failure or neglect of the aforesaid responsibility shall constitute sufficient grounds for the filing of appropriate administrative, civil and/or criminal proceedings against the erring officers, administrators, and/or individuals.

---

[9] Zeus Keravala, What is Transport Layer Security(TLS)?, available at https://www.networkworld.com/article/2303073/lan-wan-what-is-transport-layer-security-protocol.html, last accessed on March 24, 2020.

[10] N.B.: Configuration or migration of existing web servers (Apache/Nginx, etc.) to the updated version of the TLS protocol is necessary because the Secure Sockets Layer (SSL) 3.0, TLS 1.1 and 1.2 has been superseded by TLS 1.3. Pls. see the following references on the installation of TLS 1.3 protocol:

a. The Transport Layer Security (TLS) Protocol Version 1.3 https://tools.ietf.org/id/draft-ietf-tls-tls13-23.html
b. Enable TLS Version 1.3 on Web Server https://www.ssl.support/blog/steps-to-enable-tls-1-3-on-servers/
c. How to Enable TLS 1.3 in Apache and Nginx https://www.tecmint.com/enable-tls-in-apache-and-nginx/

[11] Examples are GoDaddy, Comodo Group, DigiCert, Verisign, CAcert.org, and the like.

Section 3. Use of Future Versions of TLS or other Cryptographic Protocols.— Nothing in this Circular shall be construed to preclude the Philippine government and its instrumentalities from adopting, utilizing, and implementing such further updates or versions of the TLS or such other cryptographic protocols that are proven in accordance with the prevailing IT due diligence and best practices to have better or superior functions and features in terms of cybersecurity, privacy, and data integrity.

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

Let copies of this Circular be likewise posted and published in the official DICT website and bulletin boards, as well as in a newspaper of general circulation, if available in light of the public health emergency.

GREGORIO B. HONASAN II
Secretary

Digitally signed by Reyes Jose Carlos Padicio
Date: 2020.04.13 15:31:53 +08'00'

Copy furnished:
All concerned.

D.I.C.T.
RECORDS SECTION
CERTIFIED COPY
ADRIANA A. OBLIGACION
Administrative Officer IV
5/15/2020

DICT Building, C.P. Garcia Avenue Diliman, Quezon City 1101, Philippines
+632 8920 0101 | www.dict.gov.ph