



REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY

MEMORANDUM CIRCULAR NO. **007**

FOR : ALL CRITICAL INFOSTRUCTURE(CII) OWNERS AND OPERATORS, GOVERNMENT AGENCIES, BUSINESS SECTORS AND ALL OTHERS CONCERNED

FROM : RODOLFO A. SALALIMA
Secretary

SUBJECT : PRESCRIBING THE POLICIES, RULES AND REGULATIONS ON THE PROTECTION OF INDIVIDUALS STIPULATED IN THE NATIONAL CYBERSECURITY PLAN (NCSP) 2022

DATE : 1 AUGUST 2017

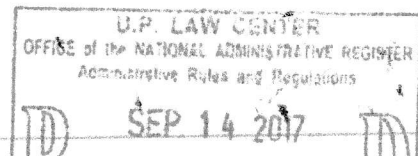
Section I. References

- 1.1. Section 2(c) of R.A. No. 10844 mandates the DICT to ensure the universal access to quality, affordable, reliable and secure services; and
- 1.2. Section 2(l) To ensure the rights of individuals to privacy and confidentiality of their personal information; and
- 1.3. Section 2(m) To ensure the security of critical ICT infrastructures including information assets of the government, individuals and businesses; and
- 1.4. Section 2(n) To provide oversight over agencies governing and regulating the ICT sector and ensure consumer protection and welfare, data privacy and security, foster competition and the growth of the ICT sector.

Section II. Definition of Terms

CyberSecurity – is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.

Critical Information Infrastructure or Critical Infostructure (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 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 matters. 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.



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

Information System – applications, services, information technology assets or other information handling components.

National Security System (NSS) – means any information system including telecommunication system used or operated by any organization or outsourced to a third party. The function, operation or use of which:

- a) Involves intelligence activities;
- b) Involves cryptologic activities related to national security;
- c) Involves command and control of military forces;
- d) Involves equipment that is an integral part of a weapon or weapons system; or
- e) Is critical to the direct fulfillment of military or intelligence missions.

Traffic Light Protocol (TLP) - is a set of designations developed by the Forum of Incident Response and Security Teams (FIRST) used to ensure that sensitive information is shared with the appropriate audience.

Section III. Background

This Memorandum Circular which covers all CII owners and operators, government agencies, business sectors and all others concerned is being issued to prescribe the policies, rules and regulations on the protection of government agencies stipulated in the NSCP 2022. The NSCP 2022, attached herewith, is approved and adopted as the national framework that will guide and institutionalize the implementation of information security governance in the country. The vision of the NSCP 2022 is for our country to have a “trusted and resilient infostructure.” To accomplish this, the following objectives are to be fulfilled:

- a) To systematically and methodically harden the CIIs for resiliency;
- b) To prepare and secure government infostructure;
- c) To raise the awareness in the business sector on cyber risks and use of security measures among businesses to prevent and protect, respond and recover from attacks; and
- d) To raise the awareness of individuals on cyber risks as they need to adopt the right norms of Cybersecurity

Section IV. General Policy

In order to protect our citizen in the online world, a Program on CyberSecurity Education and Awareness shall be developed and implemented by all agencies of the government in coordination with other private organizations with the following components:

A. Integration of CyberSecurity Courses in the Education Sector

The Academic Sector shall create Technical Working Groups (TWG) to review existing curriculum and develop CyberSecurity courses, CHED in coordination with SUCs and Private Universities/Colleges shall integrate this cybersecurity courses in the curriculum of Engineering, Computer Science, Information Technology, Law, Criminology and other

interdisciplinary programs that are projected to be of relevance to improve CyberSecurity of the country. The implementation of such curriculum shall be adopted within the year. The TESDA and DepEd shall include subjects related to Cybersecurity as identified by the TWGs to be created. A member from DICT shall seat as member of the TWGs.

B. Training of Trainers (ToT) and Certifications

Private and Academic Sectors shall continually conduct periodic Training of Trainers program in order to develop skilled CyberSecurity trainers. These pool of trainers shall be required to cascade CyberSecurity Programs at their respective agencies and areas of responsibilities and attend continuing professional education activities in CyberSecurity conducted by the DICT CyberSecurity Bureau and other certifying partners.

C. #PRInT (Paper, Radio, Internet(Social Media) and Television);

All government agencies, law enforcement, prosecution service, SUCs, private colleges and universities, media sectors and other concerned institution and organization shall contribute and assist the DICT in the conduct of this Cybersecurity Outreach Programs.

D. Observance of CyberSecurity Awareness Week

CyberSecurity Awareness Month shall be held every first week of October of each year. All relevant agencies shall observe the said CyberSecurity Week in order to promote awareness and showcase current research and development, threats and vulnerabilities, information sharing and all other activities related to CyberSecurity.

E. Philippines Government Websites

All official government websites shall be required to include CyberSecurity Awareness related content. Issues and concerns relative to the content shall be addressed within the agency, matters requiring further assistance may be referred to the DICT CyberSecurity Bureau.

Section V. Funding for the Implementation of the NCSP 2022

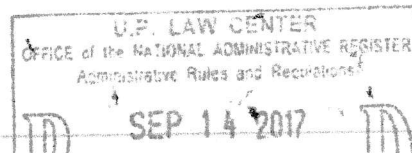
All government agencies are required to include the funding for compliance in their annual appropriations including the Information Systems Strategic Plan (ISSP) pursuant to EO 265, s.2000, and all other programs related to cybersecurity.

Section VI. Timeframe for Compliance

CIIs covered by this order shall comply within six (6) months from the signing of this Order.

Section VII. Repealing Clause

All issuances, orders, rules and regulations or parts thereof which are inconsistent with the provisions of this Memorandum Circular are hereby repealed, amended or modified accordingly.

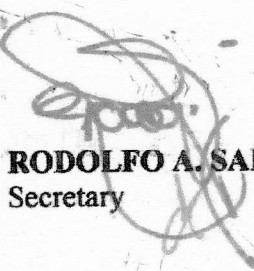


Section VIII. Separability Clause

Should any provision of this Memorandum Circular be declared invalid or unconstitutional, the other provisions not affected thereby shall remain valid and subsisting.

Section IX. Effectivity

This Memorandum Circular shall take effect upon submission of three (3) certified true copies to the University of the Philippines Law Center and/or publication in a newspaper of general circulation.


RODOLFO A. SALALIMA
Secretary

