Republika ng Pilipinas
KAGAWARAN NG KATARUNGAN
Department of Justice
Manila

VNA-DC-011

DEPARTMENT CIRCULAR NO. 010

SUBJECT : Internal Department Guidelines on Policies, Rules and Regulations on the Protection of Government Agencies Stipulated in the National Cybersecurity Plan (NCSP) 2022

DATE : FEB 13 2018

In line with Memorandum Circular No. 006, s. 2017, of the Department of Information and Communications Technology (DICT) on the above-captioned subject (copy attached), the following internal guidelines for the Department and constituent/attached agencies are hereby issued:

1. The unit or personnel directly in charge of information and communications technology (ICT) systems, infrastructure and resources shall serve as the Computer Emergency Response Team (CERT) in every agency, subject to further determination of specific personnel if necessary;

2. The head and/or particular members of the CERT shall form part of the Data Breach Response Team created as part of the agency's Security Incident Management Policy required by National Privacy Commission (NPC) Circular No. 16-03, re: Personal Data Breach Management, pursuant to the Data Privacy Act of 2012 and Implementing Rules and Regulations;

3. Respective agency heads, assisted by a senior official in charge of the ICT unit (as the CERT), shall act as Cybersecurity Officer and shall be responsible for implementation of the subject DICT Memorandum Circular;

4. Programs, projects, activities and resources necessary for implementation of NCSP 2022 shall be included in the Information Systems Strategic Plan submitted to and approved by the DICT, and in annual agency budget proposals and expenditure programs; and

5. Cybersecurity arrangements, policies and measures involving personal data shall form part of the privacy impact assessment, privacy/data protection policies, and control framework for data protection required under NPC Circular No. 16-01, re: Security of Personal Data in Government Agencies, subject to further guidance from the DICT, NPC and this Department.

This Circular takes effect immediately.

For guidance and compliance.

Department of Justice
CN : 0201802093

VITALIANO N. AGUIRRE II
Secretary

REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

MEMORANDUM CIRCULAR NO. 006

FOR	:	**ALL GOVERNMENT AGENCIES**
FROM	:	**RODOLFO A. SALALIMA** Secretary
SUBJECT	:	**PRESCRIBING THE POLICIES, RULES AND REGULATIONS ON THE PROTECTION OF GOVERNMENT AGENCIES 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 Techonology (ICT) – refers to the totality of electronic means to access, create, collect, store, procees, 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 government agencies is being issued to prescribe the policies, rules and regulations on the protection of government agencies stipulated in the NSCP 2022. The NCSP 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 NCSP 2022 is for our country to have a "trusted and resilient infostructure." To accomplish this, the following objectives should be fulfilled:

a) To systematically and methodically harden the government agencies 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

A) ESTABLISHMENT OF GOVERNMENT COMPUTER EMERGENCY RESPONSE TEAMS (GCERT)

All government agencies and instrumentalities shall establish their own CERT in accordance to DICT's rules and procedures. This CERTs shall respond to cyberattacks, particularly targeted ones that are apparently aimed at stealing, damaging, or altering information. They will take government-wide, multi-layered measures based on the assumption of a cyberattack. In promoting these measures, the Government will ensure that they are in compliance based on common internationally accepted standards, and will conduct risk analysis on its administrative responsibilities to optimize these measures.

B) COLLABORATION WITH LOCAL AND INTERNATIONAL LINKAGES

GCERT shall collaborate with local linkages for sharing of information. For purposes of systematic coordination among CERTs, international collaboration shall be coursed only through the NCERT.

C) PRIVACY OF PERSONAL DATA

The security and privacy of personal data and agreements on sharing of personal data involving government agencies or a third party shall be in conformance with the issuances from the National Privacy Commission.

D) RESPONSIBILITY OF AGENCY HEADS

Agency and other organization heads shall act as the organization's Cybersecurity Officer (CYSO) and shall be held responsible for the implementation of the provisions of this Memorandum Circular in their respective offices.

E) MONITORING AND EVALUATION OF COMPLIANCE TO THE NCSP 2022

Government agencies and its instrumentalities shall be subjected to a monitoring and evaluation system established by DICT to determine the level of their respective compliance to the NCSP 2022.

F) ORGANIZATIONAL MEMBERSHIP

The CYSOs shall create an organization headed by a chairman to be elected among member agencies. The chairman shall then report to the DICT on a periodic basis. An annual conference shall be held for all CYSOs for purposes of information sharing.

Section V. Funding for the Implementation of the NCSP 2022

All government agencies identified as CIIs are required to shoulder their expenses for compliance to this Memorandum Circular, including the Information Systems Strategic Plan (ISSP) pursuant to EO 265, s.2000, and all other programs related to cybersecurity. Said government agencies shall include in their annual budget the said expenses.

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

DOT-DOST-2017-0167