REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

MEMORANDUM CIRCULAR NO. 005

FOR	:	**ALL CRITICAL INFOSTRUCTURE(CII) SECTORS AND OTHER AGENCIES CONCERNED**
FROM	:	**RODOLFO A. SALALIMA** Secretary
SUBJECT	:	**PRESCRIBING THE POLICIES, RULES AND REGULATIONS ON THE PROTECTION OF CRITICAL INFOSTRUCTURE (CII) 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 forees;
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 CIIs and other relevant sectors is being issued to prescribe the policies, rules, and regulation on the protection of CII as stipulated in the NCSP 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 aim of the NCSP 2022 is for our country to have a "trusted and resilient infostructure." To accomplish this, the following objeetives should 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

A. Adoption of PNS ISO/IEC 27000 Family of Standards and other relevant International Standards for Mandatory Compliance

Government agencies are hereby ordered to adopt the Code of Practice stipulated in PNS ISO/IEC 27002 (Information Technology – Security Techniques – Code of Practice for Information Security Controls) within the year of effectivity of this Memorandum Circular for compliance.

The Philippine National Standard (PNS) on Information Security Management System (ISMS) ISO/IEC 27001 shall be implemented for mandatory compliance by all CII operators within two (2) years of the effectivity of this Memorandum Circular.

Other sectors not classified as CII shall adopt the PNS ISO/IEC 27002 on voluntary basis.

B. Conduct of Annual Risk and Vulnerability Assessment

All CIIs are required to participate in the conduct of risk and vulnerability assessment by the DICT at least once a year. This assessment includes overall process of identification, analysis and evaluation of weaknesses of an asset or control that can be exploited by one or more threats *(based on ISO 27000 and ISO 31000)*.

C. Conduct of Security Assessment

All CIIs are required to participate in the conduct of a security assessment program of the DICT at least once a year. This security assessment includes security evaluation of operational systems *(based on ISO/IEC TR 19791:2010)*.

D. Creation of CERT

All identified CIIs shall create its own CERT. DICT shall handle the Philippine National CERT (NCERT) which shall be the central authority for all Sectoral and Organization level CERTs in the country. All cybersecurity incidents shall be reported within 24 hours from detection to the NCERT. Information sharing shall be done with the use of established communication protocol using at the minimum the Traffic Light Protocol (TLP) to ensure that information is shared only with the appropriate audience or recipient. TLP employs four (4) colors to indicate expected sharing boundaries to be applied by the recipient(s) as defined according to the Forum of Incident Response and Security Teams (FIRST) Standard Definitions and Usage Guidance.

Traffic Light Protocol (TLP)

Color	When should it be used?	How may it be shared?
TLP:RED **Not for disclosure, restricted to participants only.**	**Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.**	**Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged**

		verbally or in person.
TLP:AMBER Limited disclosure, restricted to participants' organizations.	**Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.**	**Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN Limited disclosure, restricted to the community.	**Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.**	**Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.**
TLP:WHITE Disclosure is not limited.	**Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.**	**Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.**

E. Certificate of CyberSecurity Compliance

All CIIs shall secure a Certificate of CyberSecurity Compliance to be issued by the DICT. Basis for compliance will be, but not limited to, the criteria stipulated in the relevant edition of ISO/IEC 15408 (Information Technology -- Security Techniques -- Evaluation Criteria for IT Security) and ISO/IEC 18045 (Information Technology -- Security Techniques -- Methodology for IT Security Evaluation) as reference standards.

F. Telecommunications Cyber Hygiene

All telecommunications operators and ISPs shall conduct Cyber Hygiene activities. This includes monitoring and cleaning of their networks, including their clients, from malwares and botnets. The said telco operators are required to submit threat and compliance reports monthly.

G. Seal of CyberSecurity

All CII websites shall obtain the Seal of Cybersecurity (SCS) from the DICT upon compliance to prescribed requirements. *(Guidelines will be issued separately and will be updated as soon as the need arises.)*

H. Preparation of the Disaster Recovery and Business Continuity Plans

All organizations covered by this Memorandum Circular are hereby ordered to include the development and implementation of Disaster Recovery Plan (DR Plan) and Business Continuity Plan (BCP) as part of their ICT programs. Such plans shall be tested periodically depending on the nature of the business.

I. Conduct of National Cyber Drills and Exercises

A national cyber drills shall be conducted at least once a year by the DICT to be participated by all identified CII, both from the government and private sectors.

J. Privacy of Personal Data

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

K. Monitoring and Evaluation of Compliance to the NCSP 2022

Agency and other organizations shall be subjected to a monitoring and evaluation system established by DICT to determine the level of their respective compliance to the NCSP 2022.

L. Creation of Sectoral CERT

All CIIs shall create a Sectoral CERT to be headed by a chairman and elected among member organizations within their respective sector. The chairman shall then report to the DICT on a periodic basis. An information sharing platform shall be established among member organizations.

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 its effectivity.

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