REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

DEPARTMENT CIRCULAR NO. 003
9-06-2020

RE : SUPPLEMENTING THE DICT MEMORANDUM CIRCULAR NOS. 005, 006, AND 007, SERIES OF 2017, AND POLICIES, RULES AND REGULATIONS ON THE IMPLEMENTATION OF THE NATIONAL CYBERSECURITY PLAN 2022

WHEREAS, the Department of Information and Communications Technology (DICT) previously issued Memorandum Circular Nos. 005, 006, and 007, Series of 2017 prescribing the policies, rules and regulations on the implementation of the National Cybersecurity Plan 2022;

WHEREAS, the Philippines ranks among the top countries in the world as at most risk of online infections, and most attacked in terms of Simultaneous, Systemic, and Coordinated malicious attacks that, if left unprotected, would result to further data loss and more severe security breaches;

WHEREAS, the DICT is mandated to protect the security of consumers and business users in ICT-related matters,[1] and to render technical assistance to other government agencies on ICT-related enforcement and administration of laws, standards, rules and regulations,[2] all in line with the State's policy to secure critical ICT infrastructures including information assets of the government, businesses, and individuals;[3]

WHEREAS, consistent with the State's policy to secure critical ICT infrastructures, all bureaus, offices, agencies, and instrumentalities of the Philippine Government are mandated to establish their respective Computer Emergency Response Teams (CERTs)[4] as a proactive mechanism for cyber incident response and handling of malicious online attacks and information systems vulnerabilities;

WHEREAS, the DICT established its Cybersecurity Management System, which created the Security Operations Center (SOC);

WHEREAS, the name registered with Carnegie Mellon University for the Philippine National Emergency Response Team is CERT-PH;

NOW, THEREFORE, in the public interest, and pursuant to the provisions of existing laws, rules, and regulations, this Circular is hereby issued, adopted, and promulgated.

SEC. 1. ***Establishment of the CERT-PH.*** – The National Computer Emergency Response Team Division of the Department of Information and Communications Technology (DICT) is hereby established as the Philippine National Computer Emergency Response Team

---

[1] See §6(n), Republic Act (RA) No. 10844.
[2] See §6(h), RA 10844.
[3] §2(m), RA 10844.
[4] §4, Executive Order No. 189, series of 2015.

(CERT-PH) which shall lead, manage, and oversee the various Government, Sectoral, and Organizational CERTs.

SEC. 2. ***Sectoral CERT.*** – All Critical Information Infrastructures or Critical Infostructures (CII) sectors shall be classified and supervised by their respective Lead CERT as follows:

CII SECTOR	LEAD CERT	
	AGENCY CODE	**AGENCY NAME**
Government and Emergency Services	DICT[MISS]-CERT-PH	Department of Information and Communications Technology – Management Information Systems Service
Business Process Outsourcing	DTI-CERT-PH	Department of Trade and Industry
Healthcare	DOH-CERT-PH	Department of Health
Media	PCOO-CERT-PH	Presidential Communications Operations Office
Banking	BSP-CERT-PH	*Bangko Sentral ng Pilipinas*
Financial	DOF-CERT-PH	Department of Finance
Power	DOE-CERT-PH	Department of Energy
Water	NWRB-CERT-PH	National Water Resources Board
Telecommunications	NTC-CERT-PH	National Telecommunications Commission
Transport and Logistics	DOTr-CERT-PH	Department of Transportation

Sectoral Lead CERTs shall be responsible to timely transmit reports received from their respective CII Sector to CERT-PH.

SEC. 3. ***Government CERT.*** – All government agencies and instrumentalities shall establish their respective Government CERT named in the following manner/syntax: **[Agency acronym]-CERT-PH**. All Government CERTs falling under Section 2 hereof shall report to, and be subject to the supervision of, their respective Lead CERT.

SEC. 4. ***Organizational CERT.*** – All CERTs not falling under Sections 2 or 3 hereof shall be classified as Organizational CERTs. All Organizational CERTs shall report directly to CERT-PH.

SEC. 5. ***Escalation Protocol.*** – All Government, Sectoral, and Organizational CERTs, including CII and non-CII Government CERTs, shall comply with guidelines and escalation protocols issued by CERT-PH.

SEC. 6. ***Certificate of Cybersecurity Compliance.*** – All government agencies and instrumentalities shall secure a Certificate of Cybersecurity Compliance (C3) from the CERT-PH. The C3 shall only be issued to government agencies or instrumentalities that are fully compliant with this Circular and other related departmental issuances.

On or before 30th of January of every year, the DICT shall submit a Negative List to the Office of the President on the government agencies or instrumentalities which are unable to secure the C3 within the previous Fiscal Year.

SEC. 7. ***Security Operations Center.*** – All government agencies and instrumentalities shall connect to the Security Operations Center (SOC) of CERT-PH in accordance with the timeline and procedures established by the Cybersecurity Bureau of the DICT.

SEC. 8. ***Vulnerability Assessment and Penetration Testing.*** – All government agencies and instrumentalities shall ensure the integrity and security of their respective systems to withstand an annual Vulnerability Assessment and Penetration Testing (VAPT) that may be conducted by the CERT-PH. The CERT-PH may conduct VAPT upon request by government agencies or *motu propio* conduct random VAPT as determined by the Cybersecurity Bureau.

Government agencies and instrumentalities shall address the findings of the VAPT and comply with the recommendations, as corrective actions, of the CERT-PH within the periods indicated in the VAPT report. Finding and recommendations which are not addressed shall be reported by the DICT to the Office of the President and the concerned agency designated Cybersecurity Officer/s (CYSO) may be held administratively liable as provided by applicable laws, rules and regulations, and other relevant issuances.

SEC. 9. ***Annual Risk and Security Assessment.*** – An annual risk and security assessment shall be conducted to all CIIs at least once a year or as may be determined by the DICT.

SEC. 10. ***National Cyber Drill Exercise.*** – All government agencies and instrumentalities shall participate in the annual National Cyber Drill Exercise of CERT-PH. The CERT-PH shall issue a Certification of Participation for all attending participants which shall form part of the C3 requirements.

SEC. 11. ***Cybersecurity Training.*** – All government agencies and instrumentalities shall ensure that their respective CYSOs have undergone the minimum industry standard Cybersecurity related training/s. Training certificates of CYSOs shall be submitted and form part of the C3 requirements.

SEC. 12. ***Penalty Provision.*** – Non-compliance to this Circular which result in data loss, breaches, or similar incidents may subject the CYSO responsible to administrative, civil, or criminal liability as may be provided under pertinent provisions of the Data Privacy Act of 2012 and other applicable laws, rules and regulations, and other relevant issuances.

SEC. 13. ***Repealing Clause.*** – All issuances, orders, rules and regulations or parts thereof which are inconsistent with the provisions of this Circular are hereby repealed, amended, or modified accordingly.

SEC. 14. ***Separability Clause.*** – Should any provision of this Circular be declared invalid or unconstitutional, the other provisions not affected thereby shall remain valid and subsisting.

SEC. 15. ***Effectivity.*** – This 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.

GREGORIO B. HONASAN II
Secretary

MAR 05 2020