RECEIVING COPY
CRRU-O-2024-10-294

REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

U.P. LAW CENTER
OFFICE of the NATIONAL ADMINISTRATIVE REGISTER
Administrative Rules and Regulations
OCT 29 2024
REGISTERED
ONAR Registration
TIME: BY:

DEPARTMENT CIRCULAR NO. 004
Series of 2024

OCT 22 2024

SUBJECT : PRESCRIBING THE ADOPTION OF A LAYERED SECURITY AND DEFENSE APPROACH TO DIGITAL INFORMATION SECURITY MEASURES RELEVANT TO CYBERSECURITY FOR GOVERNMENT AGENCIES

WHEREAS, Article II, Section 24 of the 1987 Philippine Constitution provides that "The state recognizes the vital role of information and communication in nation-building."

WHEREAS, under Section 2 of Republic Act (RA) No. 10844 or the Department of Information and Communications Technology (DICT) Act of 2015, it is a declared policy of the State to ensure the rights of individuals to privacy and confidentiality of their personal information; to ensure the security of critical Information and Communications Technology (ICT) infrastructures including information assets of the government, individuals and businesses; and to provide oversight over agencies governing and regulating the ICT sector and ensure consumer protection and welfare, data privacy and security, and foster competition and the growth of the ICT sector.

WHEREAS, under Section 5 of RA 10844, the DICT is the "primary policy, planning, coordinating, implementing, and administrative entity of the Executive Branch of the government that will plan, develop, and promote the national ICT development agenda."

WHEREAS, cyber incidents encountered by the public sector are becoming more prevalent and sophisticated, making the cybersecurity of government information infrastructure an urgent priority.

WHEREAS, the Philippine Development Plan 2023 - 2028 emphasizes the importance of strengthening the Nation's cybersecurity framework to protect critical infrastructure and promote digital resilience. This has been further highlighted throughout the President's State of the Nation Addresses wherein the government's commitment to enhancing cybersecurity measures to safeguard national interests and support economic growth was highlighted.

WHEREAS, Executive Order No. 58 s.2024 adopted the National Cybersecurity Plan (NCSP) 2023-2028 as a whole-of-nation roadmap for the integrated development and strategic direction of the country's cybersecurity. The NCSP aims to position the country at the cutting edge of the digital age and, by reinforcing the country's cybersecurity defense strategies, preparing the nation for possible risks that come with the new advancements brought about by digitalization.

Department of Information and Communications Technology (DICT)
General Services Division
Records and Archives Management Section
CERTIFIED TRUE COPY
CHERRY RABULAN-JACOB
Administrative Officer V (Records Officer III)
Date: 28 OCT 2024

WHEREAS, based on the available data from CERT-PH, cyber incidents are still prevalent in sectors belonging to government and emergency services, thus, making securing information infrastructure of government agencies an immediate priority against cyber threats.

NOW, THEREFORE, pursuant to public interest, the public consultations conducted by the DICT in August and September 2024, and the provisions of existing laws, rules, and regulations, this Circular is hereby issued, adopted, and promulgated.

Section 1. Purpose — This Circular aims to adopt a layered security and defense approach to promote overall cybersecurity and protect the government's information systems and critical information infrastructure from cyber threats and cyber-attacks.

Section 2. Coverage — This Circular shall apply to all national government agencies and instrumentalities under the Executive Branch, including Government-Owned and Controlled Corporations (GOCCs) and their subsidiaries, Government Financial Institutions (GFIs), Local Government Units (LGUs), and State Universities and Colleges (SUCs).

The Philippine Congress, the Judiciary, the Constitutional Commissions, and the Office of the Ombudsman are highly encouraged to adopt this Circular.

Section 3. Definition of Terms — As used in this Circular, the following terms shall be defined as follows:

a. **Critical Information Infrastructure (CII)** means a computer or a computer system located wholly or partly in the Philippines, necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in the Philippines. CIIs consist of information process and Information Communications Technology which form part of the operation of the Critical Infrastructures (CI).

b. **Critical Infrastructure (CI)** refers to any public service that owns, uses, or operates systems and assets, whether physical or virtual, vital to the country that the incapacity or destruction of such systems or assets would have a detrimental impact on national security, including telecommunications and other vital services as may be declared by the President of the Philippines.

c. **Cyber-attack** refers to an attack or attempt via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

d. **Cyber threat** refers to any circumstance or event with the potential to adversely impact operations, agency assets, or individuals through an information system via unauthorized

Department of Information and Communications Technology (DICT)
General Services Division
Records and Archives Management Section
CERTIFIED TRUE COPY
CHERRY KAPULAN-JACOB
Administrative Officer V (Records Officer III)
Date: 28 OCT 2024

access, destruction, disclosure, modification of data, and/or denial of service, or exploitation of a particular information system vulnerability.

e. **Cybersecurity** refers to the collection of tools, policies, 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.

f. **Extended Detection and Response (XDR)** refers to a proactive security solution using machine learning and behavioral analysis for advanced threat detection.

g. **Information Security** refers to protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.[1]

h. **Identity and Access Management (IAM)** refers to a cybersecurity approach allowing controlled access to resources based on user needs.

i. **Layered security** or **"defense-in-depth"** is a layered security strategy that employs a multi-faceted approach to protect information systems. By integrating people, technology, and operational processes, organizations create a series of overlapping defenses designed to thwart potential attacks. This layered approach aims to make it increasingly difficult for attackers to breach security perimeters and access sensitive data.

j. **Third-party service provider** refers to any unaffiliated person, company, or entity that performs services for a company and are paid for their services, but do not have a stake, share, or equity in the company.

Section 4. Risk Assessment — All covered agencies and institutions may conduct a risk assessment, as necessary, to determine their respective risk appetite and tolerance, which may be used as their basis for adopting the mandatory and/or optional security requirements under Section 6 and 7 of this Circular. They may request assistance from the DICT in conducting such risk assessment.

Section 5. Security Awareness and Training — All covered agencies and institutions shall adhere to the following process of educating employees about cyber threats, vulnerabilities, and best practices to protect organizational assets, which involves providing employees with the knowledge and skills they need to recognize and respond to security incidents.

a. **Cybersecurity awareness training** — Develop cybersecurity awareness programs on the latest cyber threats, cybersecurity protocols and measures. Include cybersecurity awareness in the onboarding process for new hires and as a continuing training for current staff.

[1] Computer Security Resource Center (CSRC, National Institute of Standards and Technology (NIST)

Department of Information and Communications Technology (DICT)
General Services Division
Records and Archives Management Section
CERTIFIED TRUE COPY
CHERRY RABULAN-JACOB
Administrative Officer V (Records Officer III)
Date: 28 OCT 2024

b. **Phishing and other cyber-attack simulations** — Conduct random phishing and other cyber-attack simulations to gauge user awareness and identify employees vulnerable to these attacks.

Section 6. Layered Security (Defense-in-Depth) Approach — All covered agencies and institutions shall adopt the following layered security approach and implement such policies, programs, and information security measures relevant to cybersecurity in their operations and in carrying out their functions and responsibilities:

6.1. Physical Security — involves the protection of an organization's physical facilities and assets from unauthorized access, theft, or damage. By implementing effective physical security measures, organizations can safeguard their valuable information and resources, reduce the risk of data breaches, and maintain operational continuity.

A. Mandatory

6.1.1. Perimeter Protection — Identify and control access to the physical boundaries of a building or premise. This may entail the use of physical barriers, such as fences, walls, and gates, and the deployment of security personnel.

6.1.2. Access Control — Restrict unauthorized access to sensitive areas or resources. This entails the detection and prevention of external and internal intruders from entering restricted physical areas without permission. To implement effective access control, organizations must identify restricted areas, establish identification systems, develop clear procedures, provide employee training, monitor and audit systems, and regularly review and update policies.

6.1.3. Surveillance System — Use a video surveillance system, such as a closed-circuit television (CCTV) camera, that can continuously monitor and record access to essential areas, especially those that host critical information assets.

B. Optional

6.1.4. Detection System — Install motion, sound, and contact detectors and sensors that can trigger an alarm when an intruder or unusual activity in the physical premises is detected.

The monitoring and recording of individuals to ensure the physical security of government premises shall be in compliance with all applicable laws and regulations, such as but not limited to the Data Privacy Act of 2012, its implementing rules and regulations, and relevant issuances by the National Privacy Commission (NPC).

Department of Information and Communications Technology (DICT)
General Services Division
Records and Archives Management Section
CERTIFIED TRUE COPY
CHERRY RABULAN-JACOB
Administrative Officer V (Records Officer III)
Date: 08 OCT 2024

6.2. Perimeter Security — The safeguarding of an organization's digital infrastructure from external threats which involves implementing measures to protect the boundaries of its information systems and networks. For purposes of this Circular, perimeter security focuses on cyberspace.

A. Mandatory

6.2.1. Next Generation Firewalls — A next-generation firewall expands upon the capabilities of a traditional firewall. It inspects data on a deeper level to identify and block threats from a seemingly normal-looking network traffic, which a firewall might miss. Firewalls should be configured and managed in accordance with the ISO 27000 family of standards.

6.2.2. Intrusion Detection/Prevention Systems (IDS/IPS) — These systems monitor and block suspicious activity on network-based and wireless traffic, and alert security teams when anomalies are detected.

6.2.3. Web Application Firewalls (WAFs) — A WAF specifically protects web applications from common web attacks like SQL injection and cross-site scripting (XSS).

B. Optional

6.2.4. Demilitarized Zone (DMZ) — A DMZ helps isolate critical systems from the public internet or untrusted network, providing a heightened layer of security.

6.3. Network Security — The practice of protecting computer networks from unauthorized access, use, disclosure, disruption, modification, or destruction. It involves a combination of hardware, software, and procedural measures to safeguard the confidentiality, integrity, and availability of network data and resources.

A. Mandatory

6.3.1. Data encryption — Encrypt sensitive data in transit (transmitted) and at rest (stored) to protect information confidentiality even if it is intercepted.

B. Optional

6.3.2. Network segmentation — Divide your network into smaller segments to limit the potential impact of a breach. This ensures that if one segment is compromised, others remain secure.

6.4. Endpoint Security — safeguarding of individual devices such as computers, laptops, and smartphones that are connected to a network. It involves implementing measures to

Department of Information and Communications Technology (DICT)
General Services Division
Records and Archives Management Section
CERTIFIED TRUE COPY
CHERRY KABULAN JACOB
Administrative Officer V (Records Officer III)
Date: 18 OCT 2024

prevent unauthorized access, use, disclosure, or modification of data stored on or transmitted through these devices.

A. **Mandatory**

6.4.1. Anti-virus and Anti-malware software — Install and maintain up-to-date antivirus and anti-malware software on all devices to detect and prevent malware infections.

6.4.2. Application control — Implement application control to restrict the execution of unauthorized software, preventing malicious programs from running on government devices.

6.4.3. Bring-Your-Own-Device (BYOD) security — Enforce security policy and technical controls, especially on mobile device management, to ensure that organizational resources are protected when allowing personally owned devices to be used for work-related activities.

B. **Optional**

6.4.4. Extended Detection and Response (XDR) — Implement a unified security incident detection and response platform that automatically collects and correlates data from multiple proprietary security components.

6.5. Data Security — Maintaining the security and reliability of data throughout its lifecycle. It involves implementation of essential solutions, policies, and strategies to ensure confidentiality, integrity, and availability across diverse storage, network, and endpoint environments.

A. **Mandatory**

6.5.1. Data classification — Classify data based on its sensitivity to prioritize security measures for the most critical information as defined in existing policies, such as Memorandum Circular No. 78, s.1964 on the Rules Governing Security of Classified Matter in Government Offices; DICT Department Circular No. 2017-002 or the Philippine Government's Cloud First Policy, as amended; Executive Order No. 608, s.2007 on the National Security Clearance System for Government Personnel with Access to Classified Matters, and other relevant laws, rules, and regulations.

6.5.2. Data Loss Prevention (DLP) — Implement DLP solutions to prevent the unauthorized transfer or exfiltration of sensitive data outside authorized channels.

Department of Information and Communications Technology (DICT)
General Services Division
Records and Archives Management Section
CERTIFIED TRUE COPY
CHERRY KABULAN-JACOB
Administrative Officer V (Records Officer III)
Date: 28 OCT 2024

6.5.3. Data Backups and Recovery — Regularly back up critical data and have a robust disaster recovery plan in place using various storage technologies to facilitate quick recovery in case of a cyber-attack or cyber incidents.

6.6 Application Security — the process of protecting software and devices from vulnerabilities that could be exploited by malicious actors. This involves implementing measures to prevent unauthorized access, data breaches, and other security incidents.

A. Mandatory

6.6.1. Regular Security Scanning and Testing — Identify and remedy vulnerabilities and employ application security solutions like Web Application Firewalls (WAFs) to protect against threats such as SQL injection and Cross-Site Scripting (XSS).

All covered agencies under Sec. 2 shall comply with the basic mandatory security measures within two (2) years from the date of effectivity of this Circular. The security requirements prescribed under this Circular shall also apply to third parties contracted by the government to provide security services. The covered agencies shall include in the contract with the third-party the terms and conditions including the liabilities of the third party in implementing the security measures.

Section 7. Other Measures — The following measures may also be adopted by the agency in addition to the layered security measures enumerated in the preceding section.

7.1. Vulnerability Management –This section iterates the process of identifying, assessing, and mitigating vulnerabilities in information systems. It involves a systematic approach to discovering and addressing weaknesses that could be exploited by malicious actors to compromise the security of an organization's data, applications, and infrastructure.

7.1.1. Vulnerability Assessment — Schedule regular vulnerability scans to identify potential security weaknesses in your systems and applications. Vulnerability scans may be requested from the DICT or conducted by a DICT-recognized third-party provider.

7.1.2. Patch management — Prioritize patching critical vulnerabilities identified through scans to address them quickly and minimize the attack window.

7.2. Identity and Access Management (IAM) – This section enumerates processes and technologies used to manage user identities and control access to organizational resources. This layer of security requires implementation of access control policies, user authentication and authorization, and regular access reviews to ensure that systems, applications, and data are accessed based on legitimate user needs.

Department of Information and Communications Technology (DICT)
General Services Division
Records and Archives Management Section
CERTIFIED TRUE COPY
CHERRY RABULAN-JACOB
Administrative Officer V (Records Officer III)
Date: 28 OCT 2024

7.2.1. Strong password policies — Enforce strong password policies with minimum password length of 16 characters with the combination of special characters, upper case letter, lower case letter and number or as may be advised by the DICT.

a. Password Length — enforce a minimum length for passwords. There may also be a maximum length.
b. Password Complexity — enforce password complexity rules (such as no use of a username within the password and a combination of at least eight uppercase/lowercase alphanumeric and non-alphanumeric characters).
c. Password Age — mandate the user to select a new password after a set number of days.
d. Password Reuse and History — prevent the selection of a password that has been used already. The history attribute sets how many previous passwords are blocked. The minimum age attribute prevents a user from quickly cycling through password changes to revert to a preferred).

7.2.2. Multi-factor authentication (MFA) — Implement MFA to add an extra layer of security for user log-ins, requiring a secondary verification factor beyond just a password.

7.2.3. Access reviews — Regularly review user access privileges to ensure users have only the minimum access required for their job functions:

a. Standard User Access – at least annually
b. Privilege Accounts – quarterly or more frequently
c. User Termination/Job Change – upon the end of contract/service
d. New System Access – upon granting access
e. Third-Party access – draw up Third Party Access Agreement with vendors to grant them access according to identified need or continuing need to access information on the agencies' premises.

7.3. Security Monitoring and Logging – This section covers essential components of a robust security posture. They involve the continuous observation and recording of network and system activity to detect and respond to potential threats. Additionally, monitoring and logging refers to the ongoing observation of network and system activity for signs of malicious activity or unauthorized access. This can be achieved through a variety of techniques, including:

7.3.1. Security logs – Implement consistent logging practices to record user activity, system events, and security incidents.

7.3.2. Log analysis – Analyze security logs to identify suspicious activity and potential breaches.

Department of Information and Communications Technology (DICT)
General Services Division
Records and Archives Management Section
CERTIFIED TRUE COPY
CHERRY RABULAN JACOB
Administrative Officer V (Records Officer III)
Date: 28 OCT 2024

7.3.3. Incident Response Plan – Develop an incident response plan to define how the agency will identify, contain, eradicate, and recover from cybersecurity incidents, in accordance with the National Incident Response Manual prescribed by CERT-PH.

7.3.4. Security information and event management (SIEM) – Implement SIEM solutions to collect and analyze security data from various sources across your environment for a more holistic view of security threats.

7.4. Validation Testing – A type of software testing that verifies whether a software product meets the specified requirements and satisfies the needs of its intended users. It ensures that the product is fit for the purpose and delivers the expected value.

7.4.1 Penetration Testing – Check your computer system for exploitable vulnerabilities applying best practices in software development, tools, and information systems to address security holes.

7.4.2. Secure Software Development Life Cycle (SDLC) – implement a software development methodology that incorporates security practices throughout the entire development process. It aims to ensure that security is considered and addressed from the beginning of a project to its deployment and maintenance.

Section 8. Compliance — Compliance with the minimum information security standards set forth in this Circular shall serve as a pre-requisite for the DICT's recommendation of the Information Systems Strategic Plan (ISSP)[2] of all covered government offices to the Department of Budget and Management (DBM) pursuant to Memorandum Order No. 237, series of 1989, and its amendments, if any.

Section 9. Funding — The initial funding requirements for the implementation of this Circular shall be charged against the existing budget of the covered government office and other appropriate funding sources the DBM may identify, subject to relevant laws, rules, and regulations.

Section 10. Penalty — Non-compliance resulting in a security incident shall be subjected to provisions under relevant laws, rules and regulations including but not limited to RA 10173 and RA 10175, and its future applicable amendments and laws.

Section 11. Separability Clause — If any part, section, or provision of this Circular is declared invalid or unconstitutional, the remaining provisions not affected thereby shall continue to be in full force and effect.

[2] DICT Department Circular No. 001 s. 2024, Section 10.d

Department of Information and Communications Technology (DICT)
General Services Division
Records and Archives Management Section
CERTIFIED TRUE COPY
CHERRY RA BULAN-JACOB
Administrative Officer V (Records Officer III)
Date: 28 OCT 2024

Section 12. Repealing Clause — All other circulars, departmental issues, or parts thereof that are inconsistent with this Circular are hereby amended, modified, repealed, or superseded or modified accordingly.

Section 13. Effectivity Clause — This Circular shall take effect fifteen (15) calendar days after its publication in the Official Gazette or any newspaper of general circulation and upon filing with the Office of the National Administrative Register (ONAR) of the University of the Philippines Law Center.

Let copies of this Circular be posted and published on the official DICT website and bulletin boards.

IVAN JOHN E. UY
Secretary

PRESCRIBING THE ADOPTION OF A LAYERED SECURITY AND DEFENSE APPROACH TO DIGITAL INFORMATION SECURITY MEASURES RELEVANT TO CYBERSECURITY FOR GOVERNMENT AGENCIES

Department of Information and Communications Technology (DICT)
General Services Division
Records and Archives Management Section
CERTIFIED TRUE COPY
CHERRY RABULAN JACOB
Administrative Officer V (Records Officer III)
Date: 08 OCT 2024