DSWD
Department of Social Welfare and Development

BAGONG PILIPINAS

MEMORANDUM CIRCULAR
NO. 03
Series of 2024

SUBJECT: THE DSWD CYBERSECURITY POLICY

I. RATIONALE

The Department of Social Welfare and Development (DSWD) is steadfastly committed to preserve the integrity, confidentiality, and availability of the information about the individuals and communities we are entrusted to serve. Ensuring a robust cybersecurity infrastructure is paramount in an era where digital interactions form the backbone of effective service delivery. This Cybersecurity Policy delineates the essential principles and strategies designed to fortify our digital assets and data against various cyber threats, thereby promoting a secure and resilient digital environment.

In recent years, the world has witnessed an alarming surge in cybersecurity threats, posing significant risks to individuals, organizations, and nations at large. With the increasing dependence on digital technologies, the frequency and sophistication of cyberattacks have risen exponentially. To address this pressing issue and safeguard the integrity of our digital infrastructure, the formulation and implementation of a high-level cybersecurity policy is imperative.

Through this policy, we aim to cultivate a culture of cybersecurity awareness and adherence, fostering a safeguarded digital ecosystem that propels the DSWD to fulfill its mission while maintaining the trust and privacy of our beneficiaries.

The National Cybersecurity Plan (NCSP) serves as a comprehensive and strategic roadmap aimed at enhancing cybersecurity measures throughout the various government agencies in the Philippines. This plan outlines a systematic approach to address the growing challenges and threats in the digital realm, which emphasizes the importance of safeguarding sensitive information, critical infrastructure, and the privacy of citizens.

As part of the Department's effort to align its cybersecurity initiatives with the overarching objectives of the NCSP, this policy is developed.

II. LEGAL BASES

1. The **Electronic Commerce Act of 2000 (Republic Act No. 8792)** governs electronic data exchanges, encompassing all electronic transactions with the government. It stipulates the retention,

DSWD Central Office, IBP Rd., Bataan Complex, Constitution Hills, Quezon City, Philippines 1126
Website: http://www.dswd.gov.ph Tel Nos.: 9517119 Telefax: 9319105

SOCOTEC ISO 9001
PAB

confidentiality, and utilization of electronic signatures, along with penalties for violations.

2. The **Cybercrime Prevention Act of 2012 (Republic Act No. 10175)** addresses cybersecurity offenses, such as hacking, identity theft, and unauthorized access to computer systems. The DSWD refers to this law to strengthen its cybersecurity initiatives, protect its Information and Communications Technology ICT infrastructure, and prevent cybercrime incidents that may compromise its operations and data.

3. The **Data Privacy Act of 2012 (Republic Act No. 10173)** enshrines personal data protection and individual rights regarding personal information in the Philippines. The DSWD utilizes this legislation as a basis for enforcing cybersecurity measures to secure personal data and adhere to data privacy standards.

4. The **DSWD Administrative Order 09 Series of 2015**: Policy on Stewardship, Acceptable Use and Security of The DSWD Information and Communication Technology (ICT) Resources.

5. The **National Security Policy [2023-2028] (NSP)** contains the guiding principles and interests, as well as a set of clearly defined and articulated goals aimed at protecting and promoting national security.

III. DEFINITION OF TERMS

1. **Authentication** - The process of verifying the identity of a user, device, or system before granting access to resources or data.

2. **Cybersecurity** – 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. It is the ability to protect or defend the use of cyberspace from cyber attacks.

3. **Digital Assets** - are intangible, electronically stored assets that hold economic value, a distinct usage right, or distinct permission for use, such as databases, software, code, documents, audio, videos, logos, slide presentations, spreadsheets, and websites.

4. **End-Of-Life (EOL) Product** - A product, specifically hardware or software wherein the vendor stops the marketing, selling, or provisioning of parts and services, or no longer provides security updates or bug fixes.

5. **ICT -** An abbreviation of Information and Communications Technology; the use of computers and other electronic equipment and systems for an organization's operations, including collection, storage, use, and transmission of data electronically.

6. **Information System-** refers to a system for generating, sending, receiving, storing, or otherwise processing electronic data messages or electronic documents and includes the computer system or other similar device by or which data is recorded, transmitted or stored and any procedure related to the recording, transmission or storage of electronic data, electronic message, or electronic document.

7. **Personal Information** - "Any information recorded in a material form or not, from which an individual's identity is apparent, or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual."[1]

8. **Philippine Digital Transformation Strategy -** refers to a government-led initiative aimed at harnessing digital technologies to transform various sectors of the economy and improve the delivery of public services. The DTS is part of the government's efforts to promote digitalization, innovation, and economic growth.

9. **Risk Management-** Implementation of a risk management framework to lay down the necessary controls to address any and all kinds of risks, incidents and/or compromises within the Department.

10. **Third-party vendor/service provider** - Refers to any individual, professional, or entity engaged in providing any kind/type of services with which the DSWD had an agreement, irrespective of payment arrangements or contractual stipulations.

11. **Threat** - Any potential danger or risk to a system, data, or network.

12. **Vulnerability** - A weakness in a system or application that can be exploited by attackers to gain unauthorized access, disrupt operations, or steal data.

13. **Zero Trust** - Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.

IV. OBJECTIVES

The objective of this policy is to strengthen the DSWD's commitment to preserve the integrity, confidentiality, and availability of information crucial to the individuals and communities entrusted to its care. Recognizing the paramount importance of a robust cybersecurity infrastructure in today's digitally driven service delivery landscape, this policy delineates essential principles and strategies to safeguard the DSWD's digital assets against diverse cyber threats, ensuring a secure and

[1] Data Privacy Act of 2012, Rep. Act No. 10173 § 3(g) (Aug 15, 2012) (Phil.).

resilient digital environment. Faced with a global surge in cybersecurity threats, the objective is to formulate and implement a high-level cybersecurity policy that aligns with the objectives outlined in the above legal bases. Through this policy, the DSWD aims to cultivate a culture of cybersecurity awareness, fostering a protected digital ecosystem that supports the fulfillment of its mission while upholding the trust and privacy of beneficiaries.

V. COVERAGE

This policy encompasses all individuals and entities engaged with the DSWD, directly or indirectly, in various capacities. The outlined cybersecurity measures and protocols apply to:

1. **The DSWD Personnel**: All employees, whether permanent, contractual, or temporary, must adhere to the cybersecurity guidelines detailed in this policy while accessing or interacting with the DSWD's digital resources and information systems.

2. **Contractors**: All contractors engaged by the DSWD, including Contract of Service (COS) and Job Order (JO) workers, are obligated to comply with this policy, ensuring the secure handling and processing of information while executing tasks on behalf of the DSWD.

3. **Third-Party Vendors and Suppliers**: Vendors and suppliers providing products, services, or solutions to the DSWD must adhere to the cybersecurity stipulations outlined herein, ensuring the safeguarding of the DSWD's digital assets and data they may access or interact with during their service provision.

4. **Affiliated Entities**: Any organizations or entities collaborating with the DSWD in various initiatives or projects must align their cybersecurity practices with the standards outlined in this policy while interacting with the DSWD's digital infrastructure.

5. **Digital Assets:** Digital assets, including data, software, and various forms of digital information of the DSWD shall be protected from threats, such as unauthorized access, theft, data breaches, malware, and other cyberattacks.

6. **ICT Infrastructure:** The underlying technical and physical components, systems, and networks that support an organization's information and communication technology operations, including hardware, software, networks, data centers, and other elements that are essential for the functioning of the DSWD shall be protected from threats, such as unauthorized access, theft, data breaches, malware, and other cyberattacks.

Compliance with this policy is imperative for all covered entities, ensuring collective vigilance and resilience against cyber threats, thereby preserving the integrity, confidentiality, and availability of sensitive information and digital assets under the DSWD's purview.

VI. CYBERSECURITY POLICY PRINCIPLES

These principles and strategies are meant to guide the DSWD in developing and implementing policies, standards, procedures, and technologies towards confidentiality, integrity, and availability of its digital assets and data.

1. **Shared Responsibility:** The DSWD recognizes that protecting an organization's digital assets, infrastructure, and data is a collective effort that involves various parties working together to mitigate risks and ensure a strong security posture and shall thus adopt a shared responsibility model for cybersecurity, wherein security responsibilities, accountabilities, obligations, and roles are distributed among top-level leadership, ICT and security teams, employees and end-users, system administrators and third-party vendors and contractors.

2. **Privacy by Design**: The DSWD recognizes the importance of privacy and thus integrates privacy-enhancing technologies from the design stage throughout the data lifecycle to ensure that the privacy of all kinds of data is protected and secured.

3. **Data Loss Prevention**: The DSWD recognizes the risks associated with the processing of personal and sensitive personal information within, through, and from its information systems and thus adopts a set of rules and guidelines to ensure that all data within the organization are afforded appropriate security measures to prevent or mitigate risks and vulnerabilities such as but not limited to unauthorized processing, disclosure, and access.

4. **Zero-Trust**: The DSWD recognizes that in the evolving cybersecurity landscape, threats can come from anywhere, both internally and externally. It shall thus adopt the zero-trust approach. It is a posture that assumes that no one, whether inside or outside the DSWD, should be trusted by default. Trust is never assumed, and continuous verification and authentication are required from anyone and anything trying to access resources on the network, regardless of their location. It is designed to enhance security and protect against both external threats and insider threats.

5. **Transparency and Communication**: Establish clear communication channels for reporting issues and informing stakeholders about cybersecurity policies and incidents.

6. **Least Privilege:** It is a security practice that restricts individuals or systems to the minimum level of access or permissions required to perform their tasks or functions and no more. This principle helps reduce the potential attack surface and limit the damage a security breach or a compromised account can cause.

7. **Collaboration**: Collaborate with other government agencies, private sector entities, and international bodies to stay abreast of emerging threats and best practices

8. **Legal and Regulatory Compliance**: Ensure compliance with all applicable legal and regulatory cybersecurity, data protection, and privacy requirements, including sanctions for any violations thereof.

9. **Security-by-Design**: Adopt and implement strong and scalable security protocols and ensure that baseline information and cyber security are embedded in all development lifecycles and processes of the Department.

10. **Monitoring and Auditing**: Continuously and proactively identify and assess reasonably foreseeable vulnerabilities in computer networks, and take preventive, corrective, and mitigating action against security incidents that can lead to serious legal exposure or violation of applicable laws, rules, or regulations.

11. **Risk Assessment**: Regularly conduct comprehensive risk assessments to identify and mitigate cybersecurity threats and vulnerabilities.

12. **Response and Recovery**: The DSWD recognizes the imminent threats from known and unknown sources. Thus, a need to ensure that the DSWD is well-prepared for any inadvertent events that may compromise its data and disrupt its normal operations. This can be achieved risk by having a response and recovery plan that will enable the Department to quickly recover and restore operations within the earliest possible opportunity after an attack or compromise.

13. **Incident Management**: Ensure that all incidents pertaining to any kind of information system are resolved, recorded, and evaluated by effectively determining the root cause of incidents, failures, or loopholes in the process or security and thereafter eliminate the same to prevent recurrence or detect future attacks, compromise or non-compliance.

14. **User Competency and Awareness**: The DSWD recognizes the vital role of end users in keeping all critical digital assets safe and secured. Thus, end-users should be aware of controls, standards, and best practices adopted and implemented by the organization, including the proper and efficient utilization of privacy and security tools and technologies.

15. **End-Of-Life (EOL) products:** EOL poses significant security and operational risks and, therefore, its use must be strictly controlled and limited.

VII. INSTITUTIONAL ARRANGEMENTS

The following are the roles and responsibilities of the different Office, Bureau, Sections, and Units (OBSUs) towards the implementation of this policy.

1. Chief Information Officer (CIO):

    a. Shall prescribe the operational details of this policy. These directives shall be compiled as "Information and Communication Technology (ICT) Guidance on Cybersecurity".

    b. Shall strengthen engagements with recognized organizations in the field of information and cyber security in accordance with S.O. 2828 series of 2023.

    c. Shall monitor the implementation of this policy and promote the implementation of industry best practices and international standards.

2. The Information and Communications Technology Management Service (ICTMS):

    a. Shall lead the operationalization of the ICT Guidance as directed by the CIO.

    b. Shall monitor the compliance of other OBSUs to the DSWD Cybersecurity Policy, ICT Guidance on Cybersecurity, and other relevant issuances, and recommend the necessary and appropriate action.

    c. Shall coordinate with the Strategic Communications Group for centralized messaging and communications on matters related to cybersecurity.

    d. Shall determine, procure, and ensure that the appropriate and necessary software, hardware, and systems to support the policies are implemented and maintained to adapt to the constantly evolving landscape of ICT.

    e. Shall provide the necessary technical assistance by conducting strategic planning sessions and capability-building activities to support the directives and mandates of this Policy.

3. All other OBSUs may recommend measures in operationalizing this policy, particularly those they find unique to the functions of their organization.

4. Personnel and contractors

   a. Shall adhere to this policy and other related issuances, including cybersecurity clauses and requirements in their contracts with the DSWD.

   b. Shall report any suspicious activities they encounter and participate in cybersecurity capability-building activities, and collaboration with the ICTMS and security teams.

   c. Shall be vigilant in identifying suspicious emails or messages and report them promptly to the ICTMS or security team.

5. Third-party Vendors and Suppliers

   a. Shall adhere to this policy and other related issuances, including cybersecurity clauses and requirements in their contracts with the DSWD.

   b. Shall maintain open lines of communication with the DSWD regarding emerging threats and vulnerabilities.

VIII. EFFECTIVENESS REVIEW

This section outlines the evaluation process for assessing the effectiveness of the DSWD Cybersecurity Policy. The testing of policy implementation is essential to ensure that security measures are robust and aligned with the defined objectives. Periodic testing on a sampling basis is recommended, with subsequent analysis and discussion of results.

a. The analysis will be conducted by the ICTMS, the office responsible for overseeing the assessment of the cybersecurity policy effectiveness. The ICTMS shall:

   i. Conduct a comprehensive analysis of the monthly data to identify trends, patterns, and potential areas of improvement.

   ii. Compare the results against predefined benchmarks and objectives outlined in the DSWD Cybersecurity Policy.

   iii. Prepare a detailed report summarizing the findings, including any emerging risks or vulnerabilities.

   iv. Recommend adjustments or enhancements to the cybersecurity policy based on the analysis.

b. The defined parameters of measurement will be aligned with the overall objectives of the DSWD Cybersecurity Policy, ensuring that the evaluation process remains in sync with the organization's security goals.

c. This effectiveness review process is designed to provide ongoing insights into the strengths and weaknesses of the cybersecurity measures, allowing for continuous improvement and adaptation to emerging threats and challenges.

IX. EFFECTIVITY, REPEALING, AND SEPARABILITY CLAUSES

1. This Memorandum Circular (MC) shall take effect immediately.
2. All previous issuances contrary to or inconsistent with this MC are hereby repealed, modified, or amended accordingly.
3. If, for any reason, any part or provision of this MC is declared invalid, any part or provision not affected thereby shall remain in effect.

Issued on 12-Feb - 2024, Quezon City, Philippines.

REX GATCHALIAN
Secretary

Certified True Copy
WILLIAM V. GARCIA, JR.
OIC-Division Chief
Records and Archives Mgt. Division
13 FEB 2024