

ADMINISTRATIVE ORDER

No. 02

Series of 2025

SUBJECT: DSWD DATA GOVERNANCE FRAMEWORK

I. Rationale

The Department of Social Welfare and Development (DSWD) plays a pivotal role in addressing social issues and uplifting the lives of the poor, vulnerable, and disadvantaged. To achieve this mandate, DSWD oversees over 30 programs and services that cater to millions of beneficiaries across the country. These initiatives generate vast volumes of data, including beneficiary information, financial records, program performance metrics, and administrative data. However, while this data is a strategic asset essential for evidence-based decision-making, program evaluation, and continuous service improvement, the DSWD faces significant challenges in harnessing its full potential.

One of the most pressing issues is the inefficiency and ineffectiveness of data management within the DSWD. This stems from fragmentation of databases and non-interoperability of systems across different Offices, Bureaus, Services, and Units (OBSUs). Various program management offices independently develop and maintain their own information systems, resulting in data silos. This has led to over 320 million non-unique individual records¹ stored across different OBSUs. Attempts to consolidate this data have been difficult due to data structure disparities and limited computing power². The lack of system interoperability prevents the DSWD from having a comprehensive, holistic view of its beneficiaries, hindering policy development, strategic planning, and cross-program collaboration.

Data quality issues further exacerbate this problem. Approximately 9.2 million or 3% of cumulative data records contain inconsistencies or duplicates, as identified in internal data integration efforts. These anomalies have contributed to critical operational inefficiencies, such as program leakages, inclusion/exclusion errors, and overpayments. Additionally, instances of payments to beneficiaries not listed in the Listahanan registry indicate gaps in data integrity and validation processes. These

¹ Includes multiple instances of the Listahanan, program databases of the Pantawid Pamilyang Pilipino Program (4Ps), Social Pension, Unconditional and Targeted Cash Transfer Programs (U/TCT), Sustainable Livelihood Program (SLP), Social Amelioration Program (SAP), and transactional database of the Assistance to Individuals in Crisis Situation (AICS) as reported in the presentation material on the Unified Beneficiary Database (UBD) Updates as of February 2024

² Reported in the Verification Reports of the Performance Based Conditions 1 and 2 under the Beneficiary FIRST Social Protection Project

errors not only drain public funds but also erode public trust in the DSWD 's capacity to deliver aid effectively.

Compounding these issues are data security vulnerabilities. Successful breaches have led to data loss, ransomware attacks, and unauthorized data destruction, with recovery efforts taking up to six (6) months. Such incidents disrupt operations, delay critical decision-making, and expose sensitive beneficiary information to misuse.

These challenges are further validated by the DSWD's current Data Management Maturity Level. Based on the conducted baseline assessment, the DSWD is positioned at the Repeatable maturity level, with an overall data management maturity score less than 2³. This maturity level indicates that while basic processes and practices exist, they are informal, inconsistent, and not fully integrated into the DSWD's broader organizational structure. Gaps in standardization, systematization, and coordination persist across data management practices. These deficiencies contribute to challenges in ensuring data quality, security, and optimal utilization, ultimately affecting DSWD's ability to deliver effective, efficient, and timely social welfare programs.

Recognizing the impact of these challenges, DSWD aims to institutionalize a Data Governance Framework. This framework will enforce controls across the entire data lifecycle - from creation, collection, and processing to storage, utilization, transmission, and eventual archival or disposal. It will promote standardization of data management practices, system interoperability, as well as data quality, privacy, and security. The framework is a critical enabler of DSWD's broader digital transformation strategy, which seeks to modernize service delivery, enhance inter-agency collaboration, and optimize the use of digital technologies to achieve better social welfare outcomes.

Without a unified Data Governance Framework, DSWD risks perpetuating inefficiencies, data quality inconsistencies, and security vulnerabilities, which may result in audit findings, mismanagement of funds, legal liabilities, and ethical concerns. Through the institutionalization of data governance, the DSWD will strengthen its capacity to deliver timely, data-driven social welfare and development programs, ensure the integrity of public resources, and build trust with stakeholders. This initiative is essential for modernizing DSWD's operational landscape and reinforcing its core values of being *maagap at mapagkalinga, matapat, and mahusay*.

³ Based on the Overall Data Management Maturity Assessment Baseline Report

II. Policy Statement

The DSWD is committed to the responsible, efficient, and effective management and governance of data as a vital organizational asset. This policy establishes a comprehensive Data Governance Framework to ensure that all data generated, collected, and managed by the DSWD is accurate, secure, accessible, and high-quality. The framework will facilitate the enforcement of consistent practices across the entire data lifecycle, from creation and collection to archiving and disposal.

In line with the broader strategic goals of the DSWD, this policy paves the way for data use optimization for informed decision-making, supports service delivery improvement, and safeguards the privacy and integrity of beneficiary and program-related information by promoting accountability, transparency, and compliance with relevant laws, standards, and regulations. All DSWD personnel and stakeholders are expected to adhere to this policy to uphold data governance principles that enhance efficiency, reduce redundancies, and mitigate legal and ethical risks.

III. Legal Bases

A. National Policies and Instruments

1. **National Archives of the Philippines (NAP) Memorandum Circular No. 2104-01 Series of 2021 “Electronics Records Management Policy”** provides for procedures and guidance on the management of government electronic records to ensure that such are created, maintained, circulated, and preserved or disposed of in manners consistent with statutes and issuances.
2. **Republic Act No. 11055 of 2017 “Philippine Identification System Act”** aims to establish a single national identification system for all Filipinos and resident aliens of the Philippines, thereby instituting a common identifier for all to enable a point of integration of systems and databases across the government.
3. **Executive Order No. 2, Series of 2016 “Operationalizing in the Executive Branch the People’s Constitutional Right to Information and the State Policies of Full Public Disclosure and Transparency in the Public Service and Providing Guidelines Therefor”** emphasizes the people’s right to know about matters of public concern through the Freedom of Information (FOI) Program.
4. **National Budget Circular No. 565, Series of 2015 “Results-Based Monitoring, Evaluation, and Reporting Policy”** strengthens the use of evidence-based results for decision-making and improves government performance on the delivery of goods and services for greater transparency and accountability in the allocation and use of government resources.

5. **Department of Budget and Management, Office of the Presidential Spokesperson (OPS), and Presidential Communications Development and Strategic Planning Office (PCDSPO) Joint Memorandum Circular No. 01, Series of 2015** institutionalizes the open data government policy and enjoins government agencies to develop department-wide open data policy and implement open data practices.
6. **Republic Act No. 10625 of 2013 “Philippine Statistical Act”** promotes the development of a statistical system capable of providing timely, accurate, and useful data for the government and the public.
7. **Republic Act No. 10175 of 2012 “Cybercrime Prevention Act of 2012”** provides a conducive environment for information exchange through protected systems and databases.
8. **Republic Act No. 10173 of 2012 “Data Privacy Act of 2012”** strengthens the fundamental human right of privacy, and communication while ensuring the free flow of quality information to promote innovation and growth.
9. **NAP General Circular No. 2, Series of 2009 “Guidelines on the Disposal of Valueless Records in Government Agencies”** prescribes uniform standards or guidelines to be followed by government agencies in the disposal or destruction of their valueless records through the General Records Disposition Schedule (GRDS) common to all government agencies.
10. **NAP General Circular No. 1, Series of 2009 “Rules and Regulations Governing the Management of Public Records and Archives Administration”** provides for rules and regulations to empower government agencies to better coordinate in the management of government records and public archives.
11. **Republic Act No. 9470 of 2007 “National Archives of the Philippines Act of 2007”** strengthens the system of management and administration of archival records, establishing for the purpose the National Archives of the Philippines, and for other purposes.
12. **Republic Act No. 8792 of 2000 “E-Commerce Act”** recognizes the use of ICT in official transactions of the public and of the government. This law allows the legal recognition of electronic documents and digital signatures. There are also penalties for hacking, piracy, and for other violations of this law.

B. DSWD Issuances

1. **Memorandum Circular No. 03, Series of 2024 “DSWD Cybersecurity Policy”** strengthens the DSWD's commitment to preserve the integrity, confidentiality, and availability of information crucial to the individuals and communities entrusted to its care.

2. **Administrative Order No. 02, Series of 2024 “DSWD Strategic Plan 2024-2028”** provides emphasis on the collection of performance measures to track the progress towards achieving the strategic goals of the DSWD.
3. **Memorandum Circular No. 11, Series of 2023 “DSWD Data Privacy Manual”** serves as the basis of the DSWD and its personnel in operationalizing its data protection and security measures and incorporating data privacy measures in the performance of their duties.
4. **Memorandum Circular No. 1, Series of 2023 “Amended Freedom of Information (FOI) Agency Manual”** which sets out rules and procedures in dealing with requests for information.
5. **Administrative Order No. 01, series of 2021 “DSWD Policy Agenda 2020-2025”** identifies that integrating data systems within DSWD and exploring the wealth of data, including innovative data sources, is a key sub-element under the Research and Data element of the policy theme on Enhancing governance by harnessing whole-of-government and partnerships.
6. **DSWD Administrative Order No. 08, Series of 2019 “Guidelines for the Harmonized Planning, Monitoring, and Evaluation System”** creates the Planning Monitoring and Evaluation Technical Team which shall ensure proper coordination and data sharing to effectively track the performance based on targets set in the Strategic Plan.
7. **DSWD Memorandum Circular No. 04, Series of 2014 “Guidelines in the Operationalization of the Unified Results-Based Monitoring And Evaluation System”** guides the CO-OBSUs, FOs, and attached agencies in the operationalization of the M&E system, focusing on the reporting flow, timelines, and institutional arrangements.

IV. Objectives

The DSWD Data Governance Framework is intended to establish a comprehensive and adaptive data governance system that ensures the integrity, accessibility, security, and interoperability of data throughout its lifecycle — from creation to disposal. This system will promote accountability, transparency, and ethical use of data, in line with legal, technical, and statistical standards, and it will serve as the foundation for a data-driven culture within the DSWD.

This Administrative Order specifically seeks to:

1. Develop clear, functional structures and mechanisms for the efficient and ethical management of social welfare and development data, supported by appropriate technological and human resources; and
2. Serve as the basis for developing detailed operational guidelines that will help the DSWD manage data as a strategic and protected asset, ensuring

compliance with all relevant laws, policies, and standards, while fostering data literacy and capacity across all levels of the DSWD.

V. Coverage and Applicability

This policy shall apply to all data management-related activities within the DSWD, including but not limited to data collection methods and sources, data storage systems and protocols, data processing and analysis techniques, data sharing practices, data reporting and utilization, data archiving and disposal procedures, among others, as deemed relevant to all DSWD Central Office - Offices, Bureaus, Services, and Units (CO-OBSUs), Field Offices (FOs), employees (permanent, contractual, casual and co-terminus), including contract of service workers, consultants, service providers contracted by DSWD, and external stakeholders as one of the consumers of DSWD data. Attached and supervised agencies of DSWD without an existing Data Governance Framework may adopt this framework or develop a similar one in alignment with this policy.

VI. Definition of Terms

1. **Data** - refers to a collection of facts, figures, symbols, and other modes of written expression, described or however represented which is received, recorded, transmitted, stored, processed, retrieved, or produced. It can be anything from numbers and text to images and videos. Data is the raw material used to represent information, or from which information can be derived.
2. **Data Architecture** - refers to the blueprint for managing data assets by aligning with organizational strategy to establish strategic data requirements and designs to meet these requirements.
3. **Data Assets** - refers to any valuable information or resources within an organization that can be used to create value or improve decision-making.
4. **Data Custodian** - refers to those who are responsible for managing the archiving, recovery, maintenance, and security of the data.
5. **Data Domain** - refers to high-level business grouping and categorization of data.
6. **Data Governance** - refers to the exercise of authority, control, and shared decision-making (planning, monitoring, and enforcement) over the management of data assets.
7. **Data Infrastructure** - refers to the underlying hardware, software, and network components that support the storage, processing, and analysis of data within an organization.
8. **Data Insights** - actionable pieces of information derived from data analysis that can be used to inform decision-making and improve organizational outcomes.

9. **Data Integrity** - refers to the accuracy and consistency of data over its lifecycle, retaining its essential qualities during storage, retrieval, or processing without unauthorized alteration.
10. **Data Lifecycle** - refers to the entire process a piece of data goes through, from its creation or collection to its eventual archiving or disposal.
11. **Data Management** - refers to the process of creating, storing, organizing, and maintaining the data created and collected by an organization.
12. **Data Owner** - refers to those who have approval authority for decisions about data within their domain.
13. **Data Privacy** - refers to the protection of personal information from unauthorized access, collection, use, disclosure, or processing. It ensures that individuals have control over their data and that it is handled responsibly.
14. **Data Quality** - refers to the overall fitness of data for its intended use. It covers dimensions such as completeness, consistency, accuracy, validity, uniqueness, and timeliness of data.
15. **Data Security** - refers to protecting data from unauthorized access, disclosure, alteration, or destruction. It encompasses measures to prevent data breaches, data loss, and other security threats.
16. **Data Steward** - refers to those who manage data assets on behalf of others and in the best interests of the organization. They represent the interests of all stakeholders and must take an enterprise perspective to ensure enterprise data is of high quality and can be used effectively.
17. **Data Utilization** - refers to the process of effectively using data to achieve specific goals or objectives, such as improving efficiency, reducing costs, increasing revenue, or enhancing customer satisfaction.
18. **Institutional Mechanisms** - refer to the structures, processes, and systems within the DSWD to achieve its objectives, ensure compliance, maintain governance, and support effective decision-making.
19. **Master Data** - refers to a core set of standardized data representing critical domains within an organization. It acts as a single source of truth for this data, ensuring consistency across various systems and processes.

VII. Data Governance Framework

Data Governance covers processes, policies, standards, and systems on data management that ensure the quality, consistency, usability, integrity, security, and availability of an organization's data assets. The DSWD Data Governance Framework establishes a comprehensive and functional system that guides all DSWD stakeholders in ensuring accurate, secure, and efficient management of the DSWD's data assets, thereby facilitating informed and effective decision-making. The framework is designed to be flexible and scalable, enabling DSWD to effectively

respond to new challenges and technologies, including artificial intelligence, big data, and the Internet of Things (IoT), while upholding the highest standards for data governance.

The framework outlines the overarching strategy, processes, roles, and responsibilities governing the DSWD’s data assets to support the fulfillment of the vision, mission, and strategic objectives as stipulated in its Strategic Plan. This framework adopts a hierarchical approach to Data Governance with different structures and components defined to distinctively address key “WH” questions but interconnect through a cycle of compliance monitoring (top-bottom approach) and feedback provision (bottom-up approach) across the different applicable layers.

More importantly, the framework emphasizes participatory development and implementation processes by highlighting the roles and responsibilities of the involved actors and positioning people at its center. These actors include the Data Governance Council, Technical Working Group (TWG), and other stakeholders, each holding critical responsibility for these elements.

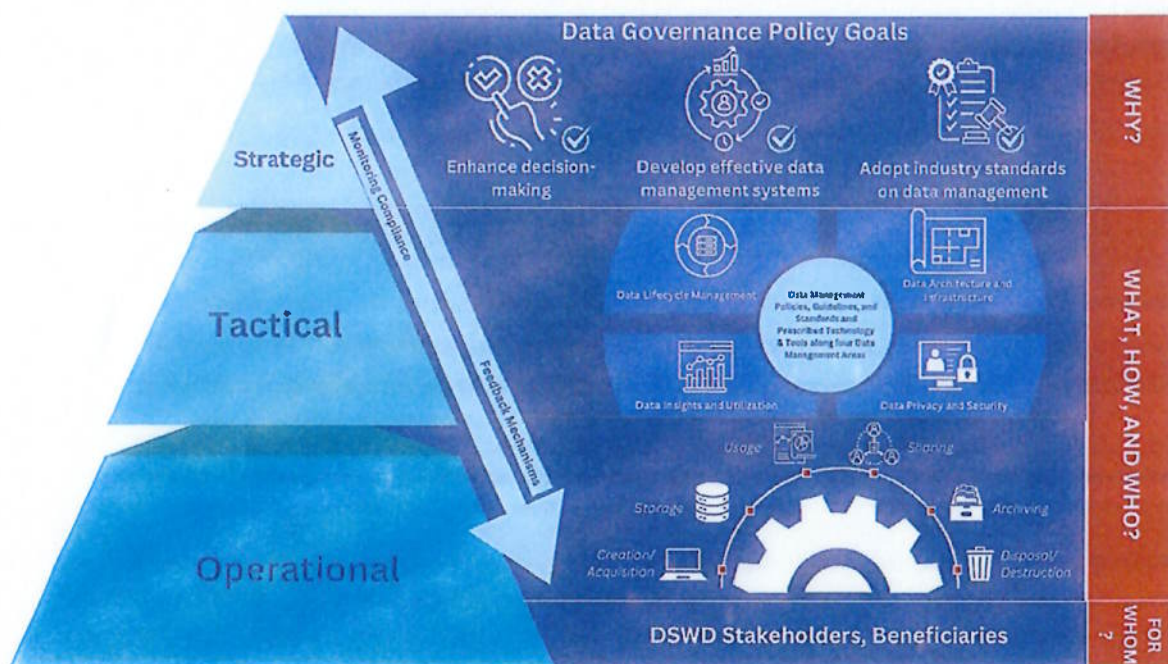


Figure 1. DSWD Data Governance Framework

The framework shows the data governance operating model encompassing three layers: Strategic Layer, Tactical Layer, and Operational Layer. This framework depicts value-driven Data Governance and begins with the question, “Why do we need data governance in DSWD?” This component of the framework represents the goals and objectives of this policy which are foundational for DSWD in fulfilling its mandate to its clients and beneficiaries. Value-driven Data Governance starts at the Strategic Layer, the topmost component, which drives and steers policy directions and data governance goals, cascading them to the lower layers. Meanwhile, the Tactical Layer, the intermediate component, translates the data governance goals into policies, standards, processes, and procedures. Lastly, the Operational Layer, the bottom

component, implements the directives laid out by the upper layers, with the intention of ultimately benefiting the stakeholders of the DSWD for whom the data governance system is being established. Meanwhile, data-related conflicts arising from the lower layers are escalated to the upper layers for proper resolution.

A. Strategic Layer: Data Governance Policy Goals

The Strategic Layer involves the high-level view of data governance goals of enhancing decision-making, developing effective data management systems, complying with regulations, and adopting industry standards on data management. This involves integrating effective data management practices into daily operations, replicating them across other government entities, and consistently applying them to drive evidence-based improvements in social welfare and development. These goals intend to support and contribute to the DSWD's strategic objectives outlined in the DSWD Strategic Plan through relevant, efficient, and reliable data and information.

This layer guides the development and implementation of elements in the tactical and operational layers, ensuring that the outcomes of these layers contribute to achieving the DSWD's data governance goals, and ultimately contributing to the attainment of the DSWD's vision, mission, and strategic objectives.

The Strategic Layer is enabled by the Data Governance Council which sets overall direction and policies for data governance. The Council defines goals and objectives that drive the development and implementation of data governance policies, standards, processes, and procedures.

The Council shall be headed by the Undersecretary for Policy and Planning Group and composed of Undersecretaries representing various clusters, and supported by External Technical Advisers.

B. Tactical Layer: Data Stewardship and Governance Enablers

The Tactical Layer provides the foundation for effective implementation and enforcement of policies, standards, and practices. This layer includes two key components – data stewardship and data governance enablers.

The *data stewardship* component of this layer encompasses the development and implementation of coherent policies, guidelines, and standards on data management. In light of this policy issuance, comprehensive operational guidelines will be subsequently issued on the date specified in the implementation plan⁴ of this issuance. The operational guidelines will be established to set standards in the following data-management areas:

1. **Data Lifecycle Management** - encompasses the entire journey of a piece of data, from its creation or collection to its eventual archiving or disposal.

⁴ To be submitted within five (5) working days upon approval of this policy

The operational guidelines will establish standards and procedures on data collection and preprocessing, data quality, data archiving, retention, and disposal, and data access and sharing.

2. **Data Architecture and Infrastructure** - establishes the blueprint for managing data assets by aligning with organizational strategy to define strategic data requirements, supported by the necessary hardware, software, and network components for effective data storage, processing, and analysis. The operational guidelines will cover standards and procedures on data architecture, data modeling and design, data storage and operations, data integration and interoperability, reference and master data, and data warehousing and business intelligence.
3. **Data Insights and Utilization** - focuses on deriving actionable information from data analysis, facilitating informed decision-making and improved organizational outcomes. The operational guidelines will address data analytics and reporting, and metadata⁵ management.
4. **Data Privacy and Security** - encompasses measures to protect data and personal information from unauthorized access, disclosure, alteration, or destruction. In light of the existing DSWD Data Privacy Manual (DPM), the Operational Guidelines of the Data Governance Framework shall refer to the DPM to maintain consistency and clarity in the organization's data management practices. This approach avoids potential conflicts that could arise from having multiple, possibly contradictory, frameworks governing data privacy and security. By aligning the Data Governance Framework with the DPM, the DSWD ensures that its data practices are not only compliant with established privacy standards but also streamlined and cohesive, enhancing overall effectiveness in achieving its strategic goals.

The Data Governance Technical Working Group (DG TWG) and the Office of the Data Privacy Officer (ODPO) will collaborate to align policies, standards, and practices to ensure seamless integration between data governance and privacy. A joint accountability framework will be developed to delineate shared and distinct responsibilities clearly, while regular reviews will be conducted to ensure consistency between the Data Governance Framework and the Data Privacy Manual and to address any conflicts or overlaps that may arise.

The data management policies, guidelines, and standards to be established shall be complied with by all DSWD CO-OBSUs, as well as Regional FOs. This layer ensures that the DSWD commits to continuous improvement by monitoring the data maturity and by being responsive to emerging demands through regular feedback and review mechanisms such as the semestral conduct of the Data Management Maturity Assessment (DMMA) and other compliance monitoring mechanisms. Thus, this layer

⁵ Metadata explains the data an organization possesses, its meaning, its classification, its origin, how it flows through the organization, how it changes over time, who is authorized to access or restrict its use, and its quality standards (DAMA International, 2017).

also draws upon the value of continuous improvement of skills, competencies, and job profiles of the DSWD's human resources.

The *data governance enablers component* of this layer includes the use of prescribed technologies and tools such as data management systems, security tools, and collaboration tools. Data governance enablers and stewards ensure that data lifecycle management meets established quality, privacy, and security standards while ensuring data accessibility and usability, which is crucial for timely decision-making and operational efficiency.

The Tactical Layer, led by the DG TWG, is chaired by the Assistant Secretary for Policy and Planning Group. Its members include Data Stewards representing all DSWD clusters. The DG TWG is responsible for leading the overall implementation and continuous improvement of the Data Governance Framework. The DG TWG shall also serve as the main communication and feedback mechanism in the Data Governance Framework. It consolidates guidance from the Strategic Layer and addresses emerging issues and concerns from the Operational Layer.

C. Operational Layer: Data Management

The Operational Layer encompasses all CO-OBSUs and FOs' daily execution and application of data management processes, using prescribed tools and technologies while ensuring compliance with established data governance policies, guidelines, and standards set by the Tactical Layer. The data management processes, covering the data lifecycle, include activities such as creation, collection, storage, processing, sharing, utilization, reporting, transmission, archiving, and disposal, among others. The actors in this layer are also responsible for upholding data privacy and security, ensuring full compliance with the DSWD's DPM.

The Operational Layer will be managed by designated Data Stewards of the DSWD within each CO-OBSU and FO. These roles will be established through the issuance of a special order, which will also define their respective duties and responsibilities.

To ensure proper handling and protection of data, the framework incorporates a structured classification system that categorizes data into confidential, internal, and public classifications. Each category comes with defined access controls, usage policies, and security measures aligned with the roles and responsibilities of the designated Data Stewards at the Operational Layer. Confidential data includes personally identifiable information (PII), sensitive case records, and financial information, which require stringent security protocols. Internal data consists of operational and administrative documents used exclusively within DSWD, while public data includes reports and statistical summaries meant for dissemination.

Other key actors involved in the Operational Layer to work closely with the designated Data Stewards include Data Owners, Data Analysts, Business Analysts, Data Engineers, Database Administrators, Compliance Officers for Privacy (COP), etc. Meanwhile, a universal monitoring and reporting system will be developed

and implemented to keep track of the day-to-day activities within the data management processes. A feedback mechanism will also be established to escalate and recommend resolutions on data-related issues.

VIII. Review, Monitoring, and Evaluation

A. Data Management Maturity Assessment

Data Management Maturity Assessment (DMMA) is an approach to assess the current data management capability by examining the existing data management processes and practices, leading to identifying areas for improvement, and thus, intending to improve the data management maturity level of an organization. It is based on a framework – a Capability Maturity Model (CMM)⁶ – that describes how characteristics of a process evolve from initial/ad hoc to optimized.⁷ In the context of the DSWD, DMMA encompasses four (4) data management areas, aligned with the major pillars of Data Governance as presented in the data stewardship component under the Tactical Layer of the Data Governance Framework, to wit: Data Lifecycle Management, Data Architecture and Infrastructure, Data Insights and Utilization, and Data Security and Privacy.

Accordingly, The DG TWG is tasked to lead the development and administration of the DMMA tool. Upon approval of this issuance, the first DMMA shall be conducted by the DG TWG Secretariat and participated by all CO-OBSUs and FOs. This aims to establish the data management maturity baseline for all the DSWD's CO-OBSUs and FOs. The baseline assessment will serve as the primary foundation for establishing data management thrusts and priorities, as well as a reference for technical assistance provision. It will also provide a basis for monitoring and evaluation through subsequent annual DMMA. Performance Metrics for DMMA, which will serve as the basis for tracking the effectiveness of the DMMA process, are outlined in Annex A.

A separate guideline for the DMMA will be developed to outline the administration of the tool across CO-OBS and FOs. This guideline will include a feedback mechanism that enables participating offices to report challenges and propose improvements based on their experiences with the DMMA process. Additionally, a communication strategy will be crafted to keep stakeholders informed about the DMMA process, including updates, compliance requirements, audit results, and performance metrics.

⁶ The Capability Maturity Model (CMM) is a structured framework that defines the stages of process maturity, enabling organizations to assess and improve their practices systematically. It describes how processes evolve across maturity levels, ranging from ad hoc and unpredictable to disciplined, standardized, and optimized operations. The CMM provides a roadmap for organizations to enhance efficiency, quality, and performance by adopting increasingly advanced practices at each maturity level (DAMA International, 2017).

⁷ Levels of Data Management Maturity according to the DAMA Data Management Body of Knowledge (DMBOK) 2nd Edition 2017: Initial/ad hoc (level 1), repeatable (level 2), defined (level 3), managed (level 4), and optimized (level 5)

B. Compliance Monitoring

The DSWD hereby establishes systematic compliance monitoring mechanisms to ensure that all data-related activities within the DSWD adhere to established data standards and guidelines. The DG TWG is responsible for overseeing the compliance monitoring process. This includes the development and implementation of compliance monitoring tools and strategies, such as, but not limited to the following:

1. Automated monitoring tools and instruction manual;
2. Compliance audits;
3. Risk management and incident reporting;
4. Recognition and incentives;
5. Action plans to address non-compliance issues, including specific steps, responsible parties, and timelines for resolution; and
6. Follow-up reviews to ensure that corrective actions have been implemented effectively and that compliance has been restored.

Data stewards in their respective CO-OBSUs and FOs are responsible for ensuring that data within their domains is managed according to the Data Governance Framework and related subsequent issuances and guidelines. They must regularly report to the DG TWG on compliance status and any issues identified through the monitoring tools prescribed by the DG TWG.

The DG TWG shall assign a rotating Internal Audit Team within the TWG composed of at most six (6) members to ensure compliance with the Data Governance Framework and related subsequent issuances and guidelines. The Data Governance Internal Audit Team will conduct periodic audits of data management practices according to an audit plan formulated by the DG TWG. The Internal Audit Team shall generate regular compliance reports to summarize monitoring activities, findings, and corrective actions taken. These reports must be reviewed by the DG TWG and shared with relevant stakeholders. They shall also maintain detailed audit logs of all monitoring activities, findings, and actions taken. These logs must be accessible for review during internal and external audits.

Once the standard data management practices within DSWD are fully established, institutionalized, and applied, the DG TWG shall explore and pursue third-party certification on standards related to data management, such as but not limited to: ISO Standards including the ISO 8000-1 (Data Quality), ISO/IEC 27001 (Information Security Management System), and ISO/IEC 38505-1 (Governance of Data), and others.

C. Policy Monitoring, Review, and Evaluation

The DG TWG shall submit an annual monitoring report of this Policy to the Policy Development and Planning Bureau (PDPB) every 10th of December of the current year. The content of the annual report shall be based on Annex F (Monitoring

Matrix for the Status of Implementation) of Administrative Order No. 15, series of 2024 or the Amendment of the DSWD Policy Development Process. To identify specific outputs and activities required to achieve the policy goals of the Data Governance Framework, the DG TWG shall develop a Strategic Results Framework to be submitted to the Data Governance Council for approval.

The PDPB shall conduct regular policy reviews and evaluations once every five (5) years, or more frequently if necessary, to ensure that the policy remains responsive and up-to-date with emerging technologies, regulatory requirements, and organizational needs. These policy reviews and evaluations will ensure that any necessary revisions are promptly reflected in the Data Governance Framework. Circumstances that may warrant more frequent reviews include, but are not limited to, significant changes in legislation, emerging trends or technologies impacting the policy, unforeseen operational challenges, or shifts in organizational priorities. These circumstances will be evaluated by the DG TWG.

IX. Institutional Mechanisms

1. Implementing Structure and Mechanisms

a. Data Governance Council

The Data Governance Council (DG Council) shall be composed of the following DSWD Officials:

- i. Chairperson:**
Undersecretary for Policy and Planning Group
- ii. Vice Chairperson:**
Chief Information Officer (CIO)
- iii. Members:**
 1. Undersecretary for Operations Group (OPG);
 2. Undersecretary for Conditional Cash Transfer Group (CCTG);
 3. Undersecretary for Innovations and Program Development Group (IPDG);
 4. Undersecretary for Regulatory Services, and Institutional Development Group (RSIDG);
 5. Undersecretary for General Administration and Support Services Group (GASSG);
 6. Undersecretary for Disaster Response Management Group (DRMG);
and
 7. Data Protection Officer (DPO).

The composition of the Council may be modified based on the DSWD organizational structure and as deemed necessary by the Chairperson, in consultation with the Council members. The Office of the Assistant

Secretary for Policy and Planning shall serve as the Council's technical secretariat.

Additionally, the Council shall invite External Technical Advisers from national government agencies⁸ and development partners⁹ to provide expert advice on existing and emerging industry standards, best practices, and regulatory compliances on data management. Accordingly, external data governance experts may be invited as resource persons, as necessary.

The DG Council, with guidance from the External Technical Advisers, is responsible for setting overall direction and policies for data governance. They shall define overarching goals and objectives that drive the development and implementation of data governance policies, standards, processes, and procedures.

Data governance concerns will be discussed and addressed during Council meetings conducted in a semi-annual manner, or as often as necessary. During the discussion of meeting agenda items, the Chairperson will preside over the meeting, and the DG Council members will have voting power in cases where issues arise that require decision points. In the event of a deadlock, the Chairperson will cast the deciding vote. If the Chairperson is unavailable, the Vice-Chairperson will assume leadership to ensure continuity in decision-making and the smooth conduct of the meeting.

b. Tactical Data Stewards

The DG TWG serves as the DSWD's primary data stewardship body within the Tactical Layer of Data Governance. The TWG consists of different coordinating data stewards, including one (1) permanent and one (1) alternate member from all the existing and emerging DSWD clusters:

- i. Chairperson:**
Assistant Secretary for Policy and Planning Group
- ii. Vice Chairperson:**
Director of Policy Development and Planning Bureau (PDPB) and
Director of Information and Communications Technology
Management Service (ICTMS)
- iii. Members:**

⁸ Such as the National Economic Development Authority (NEDA), Philippine Statistics Authority (PSA), National Privacy Commission (NPC), and the Department of Information and Communications Technology (DICT)

⁹ Such as the World Bank (WB) and the United Nations Development Programme (UNDP)

Technical staff/experts who will serve as permanent and alternate members representing all the DSWD clusters. In consideration of the evolving organizational structure of the DSWD, the composition of the DG TWG members may be updated as deemed necessary by the TWG Chairperson and Vice-Chairpersons.

The DG TWG is tasked with developing and implementing comprehensive operational guidelines and standards concerning data management areas cited in the Data Governance Framework. All DSWD CO-OBSUs and FOs shall follow these policies and standards. The DG TWG ensures ongoing improvement within the DSWD by promptly addressing emerging needs through activities such as periodic DMMA assessments, compliance monitoring and reviews, and updates of policies.

A comprehensive capacity-building plan shall be developed to enhance knowledge and increase proficiency in data governance, data management, and overall data literacy across the DSWD. Learning and development interventions for the DG TWG members will be implemented to enhance their skills, competencies, and job profiles through training and development programs. Accordingly, the learnings acquired by the TWG members shall be cascaded to their respective clusters, OBSUs, and FO counterparts.

Additionally, the DG TWG shall ensure that members are fulfilling their roles and responsibilities. It shall convene regularly, at least once every quarter, or more frequently as needed, to address emerging issues raised from the Operational Layer of Data Governance, as well as those data-related concerns arising from data audits, compliance monitoring activities, management reviews, and performance review and evaluation workshops. TWG members may also opt to invite technical staff or experts from their respective clusters if they find their presence necessary for discussing a particular issue.

iv. Secretariat:

A composite team composed of technical staff from the PDPB and ICTMS shall serve as the secretariat of the DG TWG. The secretariat team shall provide administrative, logistical, and technical support to the TWG. All technical groundwork, such as the development, review, and enhancement of data-related policies, guidelines, and standards, as well as the escalation of data-related issues, shall emanate from the technical secretariat for discussion in the TWG. Further, concerns that cannot be resolved at the TWG level shall be elevated to the Council for proper resolution.

c. Operational Data Stewards and Data Consumers

i. Operational Data Stewards

Operational data stewards and consumers, constituting the Operational Layer of the Data Governance Framework, are responsible for the daily execution and application of data management processes in line with the policies emanating from the Strategic Layer and guidelines and standards set by the Tactical Layer. They are individuals within the DSWD who directly interact with data as part of their daily tasks and responsibilities, including those who are direct or indirect users of the DSWD data. These individuals and roles include, but are not limited to, the following:

1. **Data Managers**¹⁰: They are responsible for overseeing the collection, storage, and usage of data within a CO-OBSU/FO to ensure data integrity, quality, security, and availability. They help the CO-OBSU/FO to leverage the data to make informed decisions.
2. **Operational Staff**: Their responsibilities include data collection, entry, data quality assurance, and reporting.
3. **Information Technology Staff**: Their responsibilities revolve around developing the information system and managing the archiving, recovery, maintenance, security, and sharing of data. They assume the following roles:
 - a. *Data Custodian* - They manage the storage and security of the data, with specific responsibility for maintaining, archiving, and recovering the CO-OBSU or FO datasets. They also enforce the technical security measures established in the DSWD Data Privacy Manual.
 - b. *Developer/Programmer* - Responsible for designing, developing, implementing, and maintaining the systems and applications that handle the data.
 - c. *Master Data Manager* - responsible for overseeing and maintaining the master data, as well as ensuring data integration and interoperability within the DSWD.

ii. Data Consumers

1. **Data Analysts**: They extract, process, and perform statistical analyses on large datasets. They help the CO-OBSUs and FOs in using data visualization tools to interpret complex data and provide insights derived from data to help the management make informed policy and program decisions. Data Analysts are proficient in data visualization tools and statistical software packages.
2. **Researchers**: They rely on data for program and project evaluation and other studies that intend to develop new or

¹⁰ Division Chief level

improve existing DSWD programs and projects. The DSWD encourages synergistic collaboration between researchers and data analysts for enhanced data interpretation and use in program evaluations.

3. **Digital/Traditional Media Service:** Uses data for undertaking advocacy, social marketing, and networking activities to promote social change and to nurture the DSWD's relationships with its stakeholders and the public.
4. **General Data Consumers:** They shall comply with established Data Governance policies and standards in terms of data security, privacy, access, and use, among others. They shall verify and validate data to ensure it is accurate and up-to-date before use. They play a pivotal role in the DSWD's feedback mechanism by monitoring and reporting.

2. Institutional Arrangements

- a. **Policy and Planning Group (PPG).** As the sub-cluster responsible for the fulfillment of the DSWD's roles on policy and plans development for the implementation of programs, projects, and services for the poor, vulnerable, and marginalized sectors of society, the PPG shall:
 - i. Spearhead the policy and plans development of the Data Governance Framework;
 - ii. Be on top in cases where the Secretary and the DG Council have concerns or issues on the development and implementation updates of Data Governance Framework; and
 - iii. Oversee the operationalization of the Data Governance Framework.
- b. **Office of the Chief Information Officer (OCIO).** As the lead office mandated to develop and execute a comprehensive ICT strategy aligned with the vision of the Department's Secretary towards cyber resilience and ICT innovation, the OICO shall:
 - i. Ensure alignment of data governance initiatives with the overall business objectives and IT strategy; and
 - ii. Provide guidance, technical assistance, and support to data stewards, managers, and consumers in implementing data management practices.
- c. **Office of the Data Privacy Officer (ODPO).** As the lead office mandated to ensure the compliance of data owners and stewards with the Data Privacy Act of 2012, its Implementing Rules and Regulations, issuances of the NPC, DSWD Data Privacy Manual, and other applicable laws and policies, the ODPO shall:
 - i. Ensure that the organization complies with all relevant data privacy laws, regulations, and standards;

- ii. Monitor changes in data privacy regulations and thereafter update policies and practices accordingly;
- iii. Coordinate with the Human Resource Management and Development Service (HRMDS) in setting proper controls to ensure that personnel handling personally identifiable information (PII) are accountable for protecting the personal data assigned to them;
- iv. Ensure that policies on data privacy are aligned with data governance policies and organizational objectives;
- v. Ensure compliance of COPs to set policies, standards, and guidelines on data protection, security, and privacy;
- vi. Provide technical assistance to CO-OBSUs and FOs on data privacy, as needed; and
- vii. Provide training programs for all personnel handling PII to ensure compliance with the Data Privacy Act of 2012.

d. Policy Development and Planning Bureau (PDPB). As the lead office in the development and implementation of the Department's Data Governance system, the PDPB shall:

- i. Lead the DG TWG Secretariat in the formulation, updating, implementation, enforcement, and compliance monitoring of the Data Governance Framework;
- ii. Lead the compliance monitoring of all CO-OBSUs and FOs on the Data Governance Framework, through the regular conduct of data audits, DMMA, and other pertinent monitoring activities;
- iii. Facilitate communication within the DG TWG and with relevant stakeholders regarding data governance policies, updates, and decisions;
- iv. Serve as technical oversight of all CO-OBSUs and FOs on data management, ensuring readily available data for regular auditing, reporting, and analytics;
- v. Facilitate the provision of tailored Data Governance-related technical assistance for all CO-OBSUs and FOs, as needed; and
- vi. Conduct regular review and evaluation of this policy every five (5) years, or more frequently if necessary, to ensure that the policy remains responsive and up-to-date with emerging technologies, regulatory requirements, and organizational needs.

e. Information and Communications Technology Management Service (ICTMS). As the primary provider of information and communications management, communication services, and technology solutions, to support the DSWD's social welfare and development strategies, the ICTMS shall:

- i. Along with PDPB, formulate and update the Data Governance Framework and ICT-related issuances, ensuring that all ICT initiatives are aligned with the Framework;

- ii. Act as technical data administrator responsible for managing and maintaining all infrastructures critical to SWD databases within a centralized data warehouse¹¹;
- iii. Oversee database server performance, security protocols, and backup processes, while conducting vulnerability assessments, and system monitoring to ensure the integrity, security, and efficiency of all information systems infrastructure;
- iv. Serve as the technical administrator responsible for managing and maintaining data integration systems, by ensuring smooth operations, troubleshooting issues, optimizing performance, implementing security measures, coordinating with cross-functional teams, enforcing patch management policies, overseeing software updates, and providing technical guidance to enhance integration efficiency;
- v. Provide ICT-related technical assistance to CO-OBSUs and FOs, as needed; and
- vi. Assist the PDPB in conducting compliance monitoring of all CO-OBSUs and FOs on the Data Governance Framework.

f. Administrative Service - Records and Archives Management Division (AS-RAMD). Primarily responsible for providing, maintaining, and managing logistical requirements to support the DSWD in attaining its mission and vision, the Administrative Service, specifically its Records and Archives Management Division shall:

- i. Create and enforce policies for physical and digital records management and archiving that align with issuances from the National Archives of the Philippines;
- ii. Classify, categorize, and preserve data and records according to retention schedules and security protocols in coordination with CO-OBSUs;
- iii. Coordinate with ICTMS on the execution of archiving, retention, and disposal of digital records and databases, according to approved data retention schedules and standards; and
- iv. Ensure compliance of Records Management Officers to set policies, standards, and guidelines on archiving, retention, and disposal of physical and digital records.

g. Digital/Traditional Media Service (DMS/TMS): As the offices responsible for undertaking advocacy, social marketing, and networking activities to promote social change and to nurture the DSWD's relationships with its stakeholders and the public, the DMS and TMS shall:

- i. Provide technical assistance to the DG TWG in creating advocacy materials that resonate with specific beneficiary groups or stakeholders based on generated data insights; and

¹¹ A data warehouse is a centralized repository that integrates data from various sources into a common data model. Development of such will enable DSWD to gain insights into its operations and make data-driven decisions.

- ii. Assist the DG TWG in creating communication plans to effectively popularize the Data Governance Framework, taking into consideration the specific concerns and interests of different stakeholders.
- h. Central Office-Offices, Bureaus, and Services (CO-OBSUs):** As data owners, managers, and users implementing their respective programs, projects, and services contributing to the overarching objectives of the DSWD, all CO-OBSUs shall:
- i. Have designated permanent and alternate members of the TWG to represent their respective cluster offices, ensuring participatory policy and plans development process;
 - ii. Ensure their office's and corresponding regional counterpart's implementation of and compliance with established data governance-related policies, standards, guidelines, processes, and procedures set herein and in other relevant subsequent issuances;
 - iii. Share access to information systems and databases to ICTMS for proper warehousing, vulnerability assessment, and quality assurance, and to PDPB for data audit, reporting, and analytics;
 - iv. Ensure compliance with all issuances related to securing information systems and databases;
 - v. Implement proper change management protocols and maintain an audit trail to monitor and track system changes; and
 - vi. Provide feedback and policy recommendations based on practical experience through various platforms, including compliance monitoring mechanisms, periodic DMMA reviews, and designated TWG members.
- i. Field Offices (FOs):** As primary data collectors and processors implementing programs, projects, and services in their respective regions contributing to the overarching objectives of the DSWD, all FOs shall:
- i. Ensure their office's implementation of and compliance with established data governance-related policies, standards, guidelines, processes, and procedures set herein and in other relevant subsequent issuances; and
 - ii. Provide feedback and policy recommendations based on practical experience through various platforms, including compliance monitoring mechanisms, periodic DMMA reviews, and CO-OBSU counterpart designated as TWG members.

X. Repealing Clause

All provisions of previous orders, memoranda, or issuances that are inconsistent with or contrary to the provisions of this Administrative Order are hereby repealed, amended, or modified accordingly.

XI. Effectivity

This Administrative Order shall take effect immediately upon approval and shall remain in force until it is revoked or amended.

Issued in Quezon City, Metro Manila, Philippines.


REX GATCHALIAN,
Secretary
Date: 17 MAR 2025

Certified True Copy


WILLIAM V. GARCIA, JR.
OIC-Division Chief
Records and Archives Mgt. Division

18 MAR 2025

ANNEX A

Data Management Maturity Assessment (DMMA) Performance Metrics

Area	Indicator	Indicative Target
Baseline Maturity Level Establishment	Percentage of CO-OBSUs and FOs participating in the baseline DMMA.	100% participation from all CO OBS and FOs
Maturity Level Improvement	Average improvement in maturity scores across the four data management areas (Data Lifecycle Management, Data Architecture and Infrastructure, Data Insights and Utilization, and Data Security and Privacy) from the baseline assessment to the subsequent assessments.	10% increase in overall maturity scores by the second assessment.
Action Plan Development	Percentage of identified improvement areas with corresponding action plans developed and implemented within six (6) months following the DMMA.	80% of identified areas should have actionable plans in place.
Frequency of Assessments	Adherence to the scheduled semiannual DMMA assessments (conducted every July and January).	100% completion of scheduled assessments without delays.
Training and Capacity Building	Number of training sessions conducted for staff on data management practices as a result of insights gained from the DMMA.	Conduct at least two (2) training sessions per year based on identified needs from the assessments.
Monitoring and Reporting	Percentage of units receiving technical assistance based on identified maturity gaps.	90% of units with identified needs receive appropriate technical assistance within three (3) months of the assessment
Data Quality	Reduction in the number of	10% reduction in data

Area	Indicator	Indicative Target
Improvement	data quality issues reported (e.g., duplicates, inaccuracies) in the months following the implementation of action plans.	quality issues from the preceding conduct of DMMA.
Sustainability of Improvements	Percentage of previous action items from prior DMMA's that have been fully implemented and sustained over time.	70% of previous action items should be fully implemented and maintained for at least one year.