DSWD
Department of Social Welfare and Development
BAGONG PILIPINAS

ADMINISTRATIVE ORDER
No. 03
Series of 2024

SUBJECT : GUIDELINES ON THE REGISTRATION AND USE OF DIGITAL SIGNATURES

I. Rationale

The passage of Republic Act No. 8792 or the Electronic Commerce Act demonstrates the country's shift towards digitalization, particularly the adoption of digital signature that recognizes the authenticity and reliability of digitized documents to facilitate domestic and international dealings, transactions, agreements and contracts.

Furthermore, the Socioeconomic Agenda of President Ferdinand R. Marcos Jr. promotes bureaucratic efficiency that involves digitalization of government processes and operations, with the aim of facilitating the transformation and digitalization of the whole-of-government.

Consistent with the aforecited national policies and Republic Act No. 11032 or the Ease of Doing Business and Efficient Government Service Delivery Act of 2018, the Department of Social Welfare and Development (DSWD) issued Administrative Order No. 20 s. 2019 or the "Guidelines on the DSWD Ease of Doing Business and Efficient Service Delivery" to enhance existing policies relevant in streamlining the process of delivering services.

Relevant thereto, the DSWD is committed to adopt the use of digital signature pursuant to Anti-Red Tape Authority Memorandum Circular No. 06 s. 2020 or the "Guidelines on the Issuance and/or Reinstitution of Permits and Licenses under the "New Normal."

Accordingly, the said DSWD initiatives are aimed at increasing efficiency and productivity in the delivery of services to its clients while ensuring authentication, integrity and non-repudiation of government documents. Thus, the following guidelines are hereby issued on the registration and use of digital signatures.

II. Legal Bases

A. Philippine Development Plan 2023-2028, Chapter 14, Practicing Good Governance and Improving Bureaucratic Efficiency;
B. Republic Act No. 8792, "Electronic Commerce Act";
C. Republic Act No. 11032, "Ease of Doing Business and Efficient Government Service Delivery Act of 2018";
D. Republic Act No. 10173, "Data Privacy Act of 2012";
E. Republic Act No. 10175, "Cybercrime Prevention Act of 2012";
F. Republic Act No. 9470, "National Archives of the Philippines Act of 2007"; and,
G. Executive Order No. 810 s. 2009, "Institutionalizing the Certification Scheme for Digital Signatures and Directing the Application of Digital Signatures in E-Government Services."

DSWD Central Office, IBP Road, Batasan Pambansa Complex, Constitution Hills, Quezon City, Philippines 1126
Website: http://www.dswd.gov.ph Tel Nos.: (632) 8 931-8101 to 07 Telefax: (632) 8 931-8191

III. Definition of Terms

The following terms are hereby defined for the purpose of these guidelines:

A. Agency Records Disposition Schedule – refers to a records control schedule specific to the agency in terms of organization and functions, showing the period that each record series is to remain in the office or storage area, and governing record preservation and destruction.
B. Data Protection Officer (DPO) – is a legal requirement for personal information controllers and personal information processors, under the Data Privacy Act of 2012.
C. Digital Certificate – refers to a file issued by a Certification Authority containing the user's personal information just like an ordinary identification, only in this case, it is digital that is used to encrypt, authenticate or digitally sign an email and document. It is used to verify digital signatures in electronic documents.
D. Digital Document – is a document that is digital in its form at the time of its conception or creation and has the legal effect, validity, or enforceability as any other document or legal writing.
E. Digital Signature – refers to any distinctive mark, characteristic and/or sound in electronic form, representing the identity of a person and attached to or logically associated with the digital data message or digital document or any methodology or procedures employed or adopted by a person and executed or adopted by such person with the intention of authenticating or approving an digital data message or digitized document.
F. Digitized Document – is the end result of transforming paper documents into a digital format using various tools and techniques that computer systems may use to automate processes or workflows.
G. Document Custodian – any individual designated to help the Document Controller to implement the Maintenance and Retention of Documented Information Procedures within one's Group / Center / Office.
H. Electronic Document Portal – is a system where documents or files may be uploaded to facilitate submission to audit teams upon request (i.e., for information systems audit, contract review and inspection, and data analytics).
I. Philippine National Public Key Infrastructure – refers to an infrastructure that secures communications among individuals and government agencies.
J. Private Key – is a key kept by the user on a client machine. The user must never reveal the private key to anyone, including the server (server administrator), not to compromise his/her identity. Used to decrypt data.
K. Public Key – refers to the virtual 'key' that subscribers use to secure files sent over an otherwise unsecure 'public' network like the Internet. While it is called public, it can also work in a private network setting. It is also used to encrypt data.
L. Records Officer - refers to any employee responsible for overseeing the records.
M. Subscriber – refers to an individual or entity whose name appears as the subject in a certificate and asserts that he, she or it uses the keys and certificate in accordance with the certificate policy.
N. Wet Signature – a term to describe the process of signing a physical paper document, form or contract with pen and ink.

IV. Objectives

These guidelines aim to provide standards to Offices, Bureaus and Services (OBS) in the DSWD Central Office and the DSWD Field Offices (FOs) for the use of digital signatures. Specifically, these guidelines are intended to:

A. Institute the use of digital signatures throughout the DSWD, ensuring Ease of Doing

Business (EODB) and increasing efficiency and productivity;
B. Provide uninterrupted services to the DSWD clients and stakeholders, addressing their needs in a timely manner;
C. Develop systems and mechanisms, protecting approving/signing authorities and digitized documents, pursuant to the standards issued by oversight bodies; and,
D. Set procedures in terms of registration and issuance of digital certificates, digitization of documents, and safekeeping of digitized documents.

V. Scope and Coverage

These guidelines shall apply when DSWD officials and employees issue digitized and digital documents, in lieu of paper documents wherein the wet signature of an approving/signing authority is required. Nothing in these guidelines shall be construed as prohibiting an office from issuing paper documents or a combination of paper, digitized and/or digital documents.

The approving/signing authorities are officials, employees and other authorized personnel of the DSWD who perform online transactions such as signing of memoranda, reports and other official documents based on the existing approved DSWD Manual of Delegation and Delineation of Authority.

Accordingly, these guidelines cover the following DSWD offices: Central Office, Field Offices, Centers, Residential Care Facilities and Satellite Offices. The DSWD Attached and Supervised Agencies may adopt these guidelines as reference for their own internal application.

Furthermore, these guidelines shall not apply to contracts and documents for bank and other transactions strictly requiring wet signatures, including but not limited to the following:

A. Checks;
B. Advice of Checks Issued and Cancelled;
C. List of Due and Demandable Accounts Payable – Advice to Debit Accounts;
D. Notice of Transfer Allocation;
E. Authority to Debit/Credit Account;
F. Exchange Bought Ticket;
G. Application for Manager's Check, Dollar Demand Draft Electronic Fund Transfer and Gift Check;
H. Application to Purchase Foreign Exchange; and,
I. Deposit Slip.

VI. Implementing Guidelines

A. General Policies

1. Documents of the DSWD bearing digital signatures shall be recognized as legally valid, except for documents not covered by these guidelines and pertinent laws, rules and regulations.
2. All key officials and employees of the DSWD occupying positions with Salary Grade 24 and higher, as well as those in the succession order at the Division Chief level and higher, whose signatures are necessary to perform online transactions, are required to apply for digital certificates with the Department of Information and Communications Technology (DICT).

3. The Philippine National Public Key Infrastructure (PNPKI) digital certificate issued by the DICT shall be considered as the only legally valid source of digital signatures, unless otherwise prescribed by pertinent laws, rules and regulations.
4. DSWD officials and employees shall be allowed to own and use their digital signatures, and store the same responsibly, in accordance with these guidelines.
5. Documents digitally signed by approving/signing authorities, bearing their name, date of signing, position and office, shall be treated as if such documents were originally signed.
6. A DSWD office, through its assigned document custodian or records officer, shall keep all documents with digital signatures, and ensure proper filing and retention based on Agency Records Disposition Schedule and pertinent records management policies.
7. Standard operating procedures and detailed guidelines shall be issued for process standardization and security of approving/signing authorities, in which the Data Protection Officer must certify that the digital signature implementation meets the requirements for the review and approval process.
8. The Order of succession and DSWD Manual of Delegation and Delineation of Authority shall be applied on the use of digital signatures, unless otherwise the signing of the document cannot be further delegated.

B. Documents for Digital Signing

1. Pursuant to the requirements of the EODB Law and the National Archives of the Philippines (NAP), the DSWD offices are allowed to use digital signatures for the following:

    a. Official communication between the DSWD and other entities;
    a. Accomplishment or performance reports;
    b. Clearances;
    c. Resolutions;
    d. Recommendation to Hire;
    e. Project proposals;
    f. Notice of Approved Payroll Action;
    g. Work and Financial Plan;
    h. Financial statements and its accompanying notes such as receipts, vouchers, policies, obligation request slips contracts, and other pertinent documents, including bank documents as applicable and acceptable by the bank;
    i. Leave of Absence Forms;
    j. Daily Time Records;
    k. Exit interview reports;
    l. Performance contract and review forms;
    m. Position classification papers;
    n. Capacity-building/training files and certificates;
    o. Recruitment/selection documents; and,
    p. Grievance reports.

2. Any other documents may bear digital signatures as determined by the Head of OBS in the DSWD Central Office and the FOs: provided that it is not among the excluded documents.

C. Registration, Renewal and Termination of Digital Certificates

1. The Information and Communications Technology Management Service (ICTMS) shall set the standard operating procedures for the use of digital signatures within six (6) months upon approval of these guidelines.

2. The DSWD officials and employees should renew their digital certificate in coordination with the ICTMS at least three (3) months before it expires, especially if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the subscriber's name and attributes remain unchanged.
3. Digital certificate can be requested for revocation or termination under any of the following conditions:

    a. When a verified request for revocation or termination is received by the DICT;
    b. When any of the information found in the digital certificate is changed or no longer applicable;
    c. When the private key or the media holding the private key, associated with the digital certificate is compromised; and,
    d. When the subscriber is no longer an official or employee of the DSWD due to resignation, retirement, absence without leave or termination of contract.

4. The DSWD shall request revocation or termination of a digital certificate, and when applicable, supported with a certification from the Human Resource Management and Development Service that the subscriber is already resigned, terminated or retired.

D. Digitization of Documents, Authentication and Safekeeping of Digitized and Digital Documents

1. The OBS in the Central Office and FOs shall designate a focal for scanning and uploading of digitized documents to the agency's Electronic Document Portal.
2. Each digitized document signed by the Head of OBS in the Central Office and FOs, with digital signatures, serves as an official record. Hence, uploading should be done by the assigned document custodian or records officer in accordance with the DSWD Quality Management System.
3. Said digitized documents can be authenticated by the: approving/signing authority whose digital signature is reflected in the said document; assigned document custodian or records officer; and, Overall Document Controller for official documents released to the recipient entity through the DSWD Records and Archives Management Division.
4. Digital documents signed digitally then produced in printed form have the same force and effect as if physically signed.

VII. Institutional Arrangements

A. Administrative Service

1. Review and ensure the repository of public key certificates and specimen signatures of DSWD officials and employees who are approving/signing authorities.
2. Monitor and submit a report to the Chairperson of the DSWD Task Force on Streamlining and Digitalization on DSWD officials and employees within one (1) month from the issuance of the latter's digital certificate; and,
3. Ensure that records having digital signatures are created and maintained in a secure environment that protects the same from unauthorized alteration or destruction.

B. Information and Communication Technology Management Service

1. Facilitate the processing of applications of DSWD officials and employees for digital certificate through consolidation of the forms and requirements for submission to the DICT, and assist in the enrollment and configuration of digital certificates of OBS in the Central Office and FOs;
2. Plan, assist and monitor the use of digital signatures, and implement a system together with OBS in the Central Office and FOs;
3. Supervise the system security protocols on digital signatures, and offer suggestions to ensure optimal system maintenance;
4. Ensure the procurement of hardware and software applications and licenses, catering to the large number of data banks, subject to availability of funds;
5. Ensure that all OBS in the Central Office and FOs have focal persons or representatives in the implementation of digital certificate;
6. Ensure that software and solutions implementing digital signatures adhere to the standards set in these guidelines and policies of oversight bodies; and,
7. Lead the conduct of training for designated document custodians or records officers on the Electronic Document Portal and proper archiving of digitized and digital documents.

C. Human Resource Management and Development Service

1. Monitor the list of DSWD officials and employees with digital signatures, in coordination with the ICTMS;
2. Ensure that all new DSWD officials and employees are oriented on the use of digital signatures;
3. Advise DSWD officials and employees to turn over their laptops and computers to the ICTMS for the deletion of installed digital certificate, when applying for resignation, retirement or termination of employment; and,
4. Ensure the revocation or termination of digital certificate of DSWD officials and employees who apply for resignation, retirement or termination of employment before the issuance of a certificate of clearance.

D. Financial Management Service

1. Prioritize programs, projects and services of the DSWD requesting funding for the application of digital certificate;
2. Monitor digital financial transactions based on existing laws, rules and regulations;
3. Implement controls to ensure authentication of documents, non-repudiation of the signatures, and integrity of documents; and,
4. Allocate budget and ensure availability of funds for the application of digital certificate in coordination with the ICTMS, as well as the following:

    a. Provide technical assistance to all OBS in the Central Office and FOs on the inclusion of funding allocation in their Annual Work and Financial Plan;
    b. Consolidate request for budget to be included in the General Appropriations Act; and,
    c. Ensure funding sources for hardware and software procurement to support digital signature systems and digitization and digital projects.

E. Designated DSWD Personal Information Controllers, Data Protection Officers and Compliance Officers for Privacy

1. Implement, enforce, and review DSWD policies on collecting, processing, retention, and disposal of personal information of DSWD officials and employees;
2. Ensures that all office procedures comply with data privacy rules under the DSWD Data Privacy Manual; and,

3. Recommend administrative sanctions on the misuse, misrepresentation, abuse and fraud on the usage of digital signatures.

F. Policy Development and Planning Bureau – Management Division (PDPB-MD)

1. Ensure the responsiveness of digital signature policy, in compliance with the EODB Law and other pertinent laws, rules and regulations;
2. Ensure that the digital signature policy will be reviewed to serve its function of making the government transactions efficient and with ease;
3. Incharge of capacity building activities and implement communication plan to increase awareness on the digital signature policy;
4. In collaboration with the Human Resource Management and Development Service, develop and implement a change management plan;
5. Ensure establishment of internal controls to avoid or mitigate impact of risks; and
6. Incharge of change management in congruence to this policy.

G. Legal Service

1. Recommend appropriate administrative sanctions for fraudulent use of digital signatures; and
2. Conduct administrative hearing, investigation and issue resolution.

VIII. Violation and Penalties

The violations and penalties for unauthorized issuance and use of digital certificates shall be governed by the following laws:

A. Republic Act No. 8792 or the Electronic Commerce Act of 2000, Section 33 on Penalties;
B. Republic Act No. 8484 or the (Access Devices Regulation Act of 1998), Section 10 on Penalties;
C. Republic Act No. 7394 or the Consumer Act of the Philippines, Article 40, Section E;
D. Republic Act No. 10173 or the Data Privacy Act of 2012, Chapter VIII on Penalties, Sections 25-27;
E. Republic Act No. 10175 or the Cybercrime Prevention Act of 2012, Chapter III on Penalties, Sections 8-9; and
F. Republic Act No. 6713 and its Supporting Implementing Rules and Regulations.

IX. Effectivity

This Administrative Order shall take effect immediately upon issuance. All other issuances of the DSWD inconsistent herewith are thereby deemed amended or revoked.

Issued this 21st day of February, 2024 in Quezon City.

REX GATCHALIAN
Secretary
Date: 21 FEB 2024

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