DRAFT MEMORANDUM CIRCULAR FOR COMMENTS

PROJECT NAME:	DSWD INFORMATION CLASSIFICATION POLICY (ISO/IEC 27001:2005 A.7.2.1)	DATE CREATED:	SEPT 6, 2014
DOCUMENT NAME:	DRAFT MEMORANDUM CIRCULAR	DATE LAST UPDATED:	October 7, 2016
NOTE: CHANGES TO THIS DOCUMENT MUST BE SUBMITTED TO THE OWNER/AUTHOR FOR APPROVAL.			

Version History:

VERSION NUMBER	CHANGE REQUEST APPROVED BY	REVISION DATE	AUTHOR	SUMMARY OF CHANGES
.01		9/22/2014	Felino O Castro V	Drafted MC
.02		03/29/2016	SSCare	Modded classification and Added Handling Section

DRAFT MEMORANDUM CIRCULAR FOR COMMENTS

Memorandum Circular No:
Series of 2016

Subject: **DSWD INFORMATION CLASSIFICATION AND HANDLING**

DSWD provides fast, efficient, and cost-effective electronic service delivery services for a variety of clients. It is crucial for DSWD to set the standard for the protection of information assets from unauthorized access and compromise or disclosure. Accordingly, DSWD has adopted this information classification policy as prescribed in ISO/IEC 27001:2005 A.7.2.1 to help manage and protect its information assets.

The Information Classification Policy is intended to help DSWD employees to manage and protect its information assets..

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually.

All DSWD employees share in the responsibility for ensuring that DSWD information assets receive an appropriate level of protection by observing this Information Classification policy

DSWD Managers or information 'owners' shall be responsible for assigning classifications to Information assets according to the standard information classification system presented below. 'Owners" have approved management responsibility. 'Owners' do not have property rights. Where practicable, the information category shall be embedded in the information itself.

All DSWD employees shall be guided by the information category in their security-related handling of DSWD information.

All DSWD information and all information entrusted to DSWD from third parties falls into one of four classifications in the table below, presented in order of increasing sensitivity.

Data Classification

Classification	Description	Examples
Unclassified / Public	• Information is not confidential and can be made public without any implications for DSWD. • Loss of availability due to system downtime is an acceptable risk. • Integrity is important but not vital.	• IEC materials widely distributed • Information widely available in the public domain, including publicly available DSWD web site areas • Financial reports required by regulatory authorities • Newsletters for external transmission
Confidential	• Information is restricted to management approved internal access and protected from external access. • Unauthorized access could influence DSWD's operational effectiveness, cause an important financial loss, or cause a major drop in public confidence. • The original copy of such information must not be changed in any way without written permission from the client. • The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Passwords and information on corporate security processes • Know-how used to process client information • Standard Operating Procedures used in all parts of DSWD's business • All DSWD-developed software code, whether used internally or sold to clients • Information received from clients and beneficiaries in any form for processing in production by DSWD. • Accomplished General Intake Sheets and its derivatives • Accomplished Household Assessment Forms and its derivatives • Household profiles of beneficiaies of DSWD programs and services • Social Case study reports Transaction records generated for the client by DSWD programs management offices
Private / Internal	• Information collected and used by DSWD in the conduct of its operations to employ people, to log and fulfill client orders, and to manage all aspects of finance. • Access to this information is very restricted within the DSWD. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Salaries and other personnel data • Pre-procurement documents such as TORs • Accounting data and internal financial reports • Confidential Reports of TWG Deliberation • Non disclosure agreements with clients\vendors • DSWD Work and Financial Plans • Minutes of Executive and Management Meetings

Data Handling Requirements

For each classification, several data handling requirements are defined to appropriately safeguard the information. It's important to understand that overall sensitivity of institutional data encompasses not only its confidentiality but also the need for integrity and availability. The following table defines required safeguards for protecting data and data collections based on their classification. In addition to the following data security standards, any data covered laws or regulations or contractual agreements must meet the security requirements defined by those laws, regulations, or contracts.

Security Control Category	Unclassified / Public	Confidential	Private / Internal
Access Controls	No restriction for viewing Authorization by Data Owner or designee required for modification; supervisor approval also required if not a self-service function	Viewing and modification restricted to authorized individuals as needed for business-related roles Data Owner or designee grants permission for access, plus approval from supervisor Authentication and authorization required for access Confidentiality agreement required	Viewing and modification restricted to authorized individuals as needed for business-related roles Data Owner or designee grants permission for access, plus approval from supervisor Authentication and authorization required for access
Copying/Printing (applies to both paper and electronic forms)	No restrictions	Data should only be printed when there is a legitimate need. Copies must be limited to individuals authorized to access the data and have signed a confidentiality agreement (e.g. NDA [Non-Disclosure Agreement]). Data should not be left unattended on a printer/fax Copies must be labeled "Confidential" Must be sent via Confidential envelope; data must be marked "Confidential"	Data should only be printed when there is a legitimate need. Copies must be limited to individuals with a need to know. Data should not be left unattended on a printer/fax May be sent via DSWD Mail
Network Security	May reside on a public network Protection with a firewall recommended IDS/IPS [Intrusion Detection System / Intrusion Prevention System] protection recommended.	Protection with a network firewall required. IDS/IPS protection required. Servers hosting the data cannot be visible to the entire Internet, nor to unprotected subnets like the conference halls and guest wireless networks. The firewall ruleset should be reviewed periodically	Protection with a network firewall required. IDS/IPS protection required. Servers hosting the data should not be visible to entire Internet. May be in a shared network server subnet with a common firewall ruleset for the set of servers
System Security	Must follow general best practices for system management and security. Host-	Must follow department-specific and OS-specific best practices for system management and security	Must follow University-specific and OS-specific best practices for system management and security Host-based

	based software firewall recommended	Host-based software firewall required Host-based software IDS/IPS recommended	software firewall required Host-based software IDS/IPS recommended
Virtual Environments	May be hosted in a virtual server environment All other security controls apply to both the host and the guest virtual machines	May be hosted in a virtual server environment All other security controls apply to both the host and the guest virtual machines Cannot share the same virtual host environment with guest virtual servers of other security classifications	May be hosted in a virtual server environment All other security controls apply to both the host and the guest virtual machines Should not share the same virtual host environment with guest virtual servers of other security classifications
Physical Security	System must be locked or logged out when unattended Host-based software firewall recommended	a Secure Data Center is recommended System must be locked or logged out when unattended Hosted in a Secure Data Center required Physical access must be monitored, logged, and limited to authorized individuals 24x7	System must be locked or logged out when unattended Hosted in a secure location required; a Secure Data Center is recommended
Remote Access to systems hosting the data	No restrictions	Restricted to local network or secure VPN group Unsupervised remote access by third party for technical support not allowed Two-factor authentication recommended	Access restricted to local network or VPN Remote access by third party for technical support limited to authenticated, temporary access via direct dial-in modem or secure protocols over the Internet
Data Storage	Storage on a secure server recommended Storage in a secure Data Center recommended	Storage on a secure server required Storage in Secure Data Center required Should not store on an individual workstation or mobile device (e.g., a laptop computer); if stored on a workstation or mobile device, must use whole-disk encryption Encryption on backup media required Paper/hard copy: do	Storage on a secure server recommended Storage in a secure Data Center recommended Should not store on an individual's workstation or a mobile device

		not leave unattended where others may see it; store in a secure location	
Transmission	No restrictions	Encryption required (for example, via SSL or secure file transfer protocols) Cannot transmit via e-mail unless encrypted and secured with a digital signature	No requirements
Backup/Disaster Recovery	Backups required; daily backups recommended	Daily backups required Off-site storage in a secure location required	Daily backups required Off-site storage recommended
Media Sanitization and Disposal (hard drives, CDs, DVDs, tapes, paper, etc.)	No restrictions	Shred reports Destruction of electronic media	Recycle Reports; Wipe/erase media
Training	General security awareness training recommended	General security awareness training required Data security training required Applicable policy and regulation training required	General security awareness training required Data security training required
Auditing	Not needed	Logins, access and changes	Logins
Mobile Devices	Password protection recommended; locked when not in use	Password protected, locked when not in use, Encryption used for Level 3 data	Password protected, locked when not in use

DRAFT MEMORANDUM CIRCULAR FOR COMMENTS

Effectivity

This Memorandum Circular shall take effect immediately.

Issued in Quezon City, This ____ day of _____, 20__ .

CORAZON JULIANO-SOLIMAN

Secretary