



State of Illinois
Department of Central Management Services

DATA CLASSIFICATION POLICY

Effective December 15, 2008

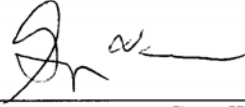
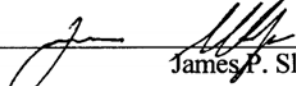
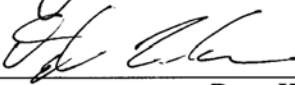
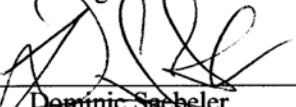
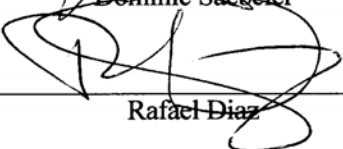
State of Illinois
Department of Central Management Services
Bureau of Communication and Computer Services

DATA CLASSIFICATION POLICY

Effective December 15, 2008

Version 1.0

APPROVAL SHEET

State CIO	 _____	Date: <u>12/15/08</u>
	Greg Wass	
CMS Director:	 _____	Date: <u>12-10-08</u>
	James P. Sledge	
CMS/BCCS Deputy Director:	 _____	Date: <u>11/20/08</u>
	Doug Kasamis	
CMS/BCCS Deputy General Counsel:	 _____	Date: <u>11/20/08</u>
	Dominic Saeheler	
CMS/BCCS Chief Information Security Officer:	 _____	Date: <u>11/20/08</u>
	Rafael Diaz	

**Please Return to: CMS/BCCS
Chief Security Office
120 W. Jefferson
Springfield, IL 62702**

Thank You.

Illinois Department of Central Management Services
Data Classification Policy

TABLE OF CONTENTS

POLICY STATEMENT

PURPOSE

SCOPE

DEFINITIONS

RESPONSIBILITY

POLICY

REVISION HISTORY

Illinois Department of Central Management Services
Data Classification Policy

POLICY STATEMENT

The State of Illinois, Department of Central Management Services, Bureau of Communications and Computer Services (CMS/BCCS) will maintain a data classification system designed to enable the use of data so that information will be protected from unauthorized disclosure, use, or modification, and deletion. The determinations to be made in accordance with this policy are subject to the requirements of state or federal law, rules or regulations.

PURPOSE

To inform State of Illinois data owners and data users about the data classification schema used by CMS/BCCS for protecting data generated, accessed, transmitted and stored by State of Illinois resources; and to promote compliance with local, state, and federal regulations regarding privacy and confidentiality of information.

SCOPE

This data classification policy is applicable to all agencies that generate, access, transmit or store information managed by CMS/BCCS.

DEFINITIONS

Definitions for terms used in this policy can be found in the BCCS Terminology Glossary located at <http://www.bccs.illinois.gov>. The terms and definitions listed below are meaningful for this policy. In the event of conflict between the definition in the BCCS Terminology Glossary and the definition contained in this policy, the definition below shall control for this Policy.

1. **Data Owner** – the individual(s) responsible for and knowledgeable about how information is acquired, transmitted, stored, deleted, and otherwise processed.
2. **Data User** – the individual(s), organization or entity that interacts with data for the purpose of performing an authorized task.

RESPONSIBILITY

1. In order to implement this policy, CMS establishes procedures and designates responsibility to specific personnel. Each Agency should also establish procedures and assign responsibility to specific agency personnel to achieve policy compliance.
2. The Data Owner is responsible for:
 - a. determining the appropriate value and classification of information generated by the owner or agency;
 - b. communicating the information classification when the information is released outside of the agency and/or State of Illinois;
 - c. communicating the information classification to CMS/BCCS and the Resource Custodian so that they may provide the appropriate levels of protection.
3. A Data User is responsible for using data in a manner that is consistent with the purpose intended and in compliance with this policy.

Data Classification Policy

4. It is the responsibility of each individual to report violations of this policy as they are brought to their attention.

POLICY

1. CMS/BCCS collects and manages data classification information to provide appropriate security and recovery measures.
2. Information must be consistently protected throughout its life cycle, from its origination to its destruction.
3. CMS/BCCS classifies data into the following three categories:
 - a. Public
 - b. Official Use Only
 - c. Confidential

DATA CLASSIFICATIONS

All information must be retained and destroyed in accordance with the State Records Act.

1. PUBLIC DATA

Public data is information that may or must be open to the general public. It is defined as information with no existing local, state, national or international legal restrictions on access or usage. Public data, while subject to State of Illinois disclosure rules, is available to all residents of the State of Illinois and to all individuals and entities external to the State of Illinois.

By way of illustration only, some examples of Public Data include:

- a. Publicly posted press releases
- b. Publicly posted meeting announcements and agendas
- c. Publicly posted newsletters and magazines.

2. OFFICIAL USE ONLY DATA

Official Use Only Data is information that must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Official Use Only Data is information that is restricted to certain employees of the State of Illinois who have a legitimate purpose for accessing such data. Data Owners and Resource Custodians may also designate data as Official Use Only.

By way of illustration only, some examples of Official Use Data include:

- a. Employment data
- b. Information stored or used by a 3rd party provider where no more restrictive confidentiality agreement exists
- c. Internal telephone books and directories

Official Use Only data:

- a. Must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure.

Data Classification Policy

- b. Must be stored in a closed container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.
- c. Must be stored in a non-publicly accessed server / drive.
- d. Must not be posted on any public website.

3. CONFIDENTIAL DATA

Confidential Data is information protected by statutes, regulations, State of Illinois policies or contractual language.

Confidential Data may be disclosed to individuals on a need-to-know basis only.

Disclosure to parties outside the State of Illinois should be authorized by executive management and/or the Data Owners and General Counsel.

Examples of Confidential Data include (but are not limited):

- a. Medical records
- b. Employee records and other non-public employee data
- c. Social Security Numbers
- d. Personnel and/or payroll or records
- e. Any data identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction.

Confidential data:

- a. When stored in an electronic format, must be protected with strong passwords and stored on servers that have protection and encryption measures in order to protect against loss, theft, unauthorized access and unauthorized disclosure.
- b. Must be stored only in a locked drawer or room or an area where access is controlled by a guard, cipher lock, and/or card reader, or that otherwise has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know.
- c. When sent via fax must be sent only to a previously established and used address or one that has been verified in a secured location.
- d. Must not be posted on any public website.

Illinois Department of Central Management Services
Data Classification Policy

Revision History

Created: November 1, 2008
Revised: N/A
Reviewed: N/A
Effective: December 15, 2008