



State of Illinois

Department of Central Management Services

DATA BREACH NOTIFICATION POLICY

Effective December 1, 2007

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

DATA BREACH NOTIFICATION POLICY

Effective December 1, 2007
Version 1.0

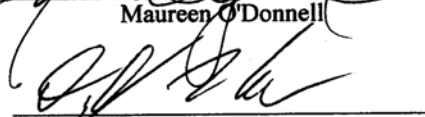
APPROVAL SHEET

CMS Director:


Maureen O'Donnell

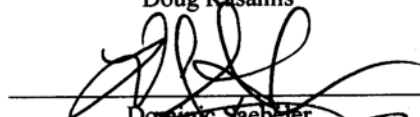
Date: 11.29.07

CMS/BCCS Deputy Director:


Doug Kasamis


Date: 10/18/07

CMS/BCCS Deputy General Counsel:


Dominic Saebler

Date: 10/18/07

CMS/BCCS Chief Security Officer:


Rafael Diaz

Date: 10/18/07

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

Thank You.

Illinois Department of Central Management Services
DATA BREACH NOTIFICATION POLICY

TABLE OF CONTENTS

POLICY STATEMENT

PURPOSE

BUSINESS CASE

RELEVANCE

SCOPE

DEFINITIONS

RESPONSIBILITY

POLICY

Illinois Department of Central Management Services
DATA BREACH NOTIFICATION POLICY

POLICY STATEMENT

It is the intent of the Illinois Department of Central Management Services (CMS) to have in place a reasonable information security policy and a Data Breach Notification Policy including procedures that address both the protection of certain information, including “Personal Information” as defined in (815 ILCS 530/5) and the prompt notification of those individuals actually or potentially affected by a breach of the security of the system data as defined in (815 ILCS 530/5).

CMS will make all reasonable efforts to protect confidential information and specifically nonpublic personal information as a “Data Collector” as defined in (815 ILCS 530/5) when it acts in that capacity. CMS will also make all reasonable efforts to protect confidential and nonpublic personal information that CMS may be managing on behalf of another state Agency that is the Data Collector.

CMS will make all reasonable efforts to protect such information under CMS control from unauthorized access, use, disclosure, deletion, destruction, damage, or removal. Though reasonable efforts are made to protect resources and data, there exists the possibility that resources and data under the control of the State may be breached. As a result, this policy requires that CMS have a reasonable and appropriate breach notification procedure or action plan in place should security procedures not prevent a breach. Such procedures should be in concert with existing laws that address notice requirements for individuals and/or entities that may actually or potentially be affected by unauthorized access or breach.

In Illinois, the Personal Information Protection Act 815 ILCS 530 outlines the requirements for notification in the event of a Breach of Personal Information.

PURPOSE

The purpose of this Policy is to recognize the importance of information security and to realize that a breach may still occur and therefore to establish a framework for addressing a breach that occurs notwithstanding the reasonable efforts to prevent such a breach.

BUSINESS CASE

State and Federal law, as well as best business practice, suggest that an organization should make reasonable efforts to secure and protect certain information that it possesses thereby protecting the integrity and confidentiality of any such maintained information. A breach of security of the protected information that occurs in spite of measures taken to protect physical and/or logical resources could result in financial loss as well as loss of customer confidence.

RELEVANCE

There are various Federal and State Laws that may apply to both security and breach situations depending upon the type of equipment, information or data that is being protected. The Illinois Statute that addresses a breach of information security is the Personal Information Protection Act 815 ILCS 530.

Illinois Department of Central Management Services
DATA BREACH NOTIFICATION POLICY

SCOPE

This Policy applies to the Department of Central Management Services (CMS) and the various Bureaus within CMS that manage, maintain, operate, store, or are otherwise active in the control of certain information that if breached would trigger notification. This Policy should also be followed by any Agency that utilizes CMS BCCS for telecommunications and technology services.

This Policy does not address human safety. Other policies, procedures, and plans address the top priority of human health and safety. These include but may not be limited to emergency (or incident) response plans, evacuation plans, personal conduct rules, emergency management plans, public health procedures, and homeland security guidelines and recommendations.

This Policy, and the procedures directed by it, address environments that require system access control, computer and operations management, system development and maintenance, physical and environmental security of information, compliance, personnel security, security organization, asset classification and control, and business continuity and response(s) to any resulting breaches of such security measures as well as other environments that handle information that must be secured.

DEFINITIONS

For purposes of this Policy, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector (specifically the State Agency that collected the information and/or the Agency that manages the equipment that houses that data).

RESPONSIBILITY

Users of state resources are responsible for following the intent of this Policy, any published associated procedure(s), and using reasonable due diligence.

Anyone observing what appears to be a breach of security, violation of this or other state policy, violation of state or federal law, theft, damage, or any action placing state resources at risk must report the incident to an appropriate level supervisor, manager, or security officer within their organization. Those reporting alleged incidents will be protected from retaliation by existing whistleblower protection laws currently enforce.

CMS staff is responsible for ensuring that appropriate and adequate protection and controls are applied to each resource under their care and identifying those that are not.

Managers and supervisors are responsible for ensuring that workers follow the intent of this Policy and are adhering to all related procedures.

Where appropriate, procedures and operational manuals that detail specific actions that implement this Policy should be created.

Procedures developed to support this Policy should be monitored and tracked for compliance with this Policy.

Illinois Department of Central Management Services
DATA BREACH NOTIFICATION POLICY

To the extent operationally feasible and cost-effective standards of responsibility will be followed as set forth in ISO 17799 and an appropriate defense-in-depth strategy.

POLICY

1. Any Agency that utilizes CMS BCCS for telecommunications and technology services should have a breach notification procedure in place that can immediately be implemented in the event of a data breach. CMS has a breach notification procedure in place titled “CMS Action Plan for Notification of a Security Breach.”
2. Any Bureau within CMS that owns or licenses computerized data that includes personal information shall disclose any “breach of the security of the system data” following discovery or notification of a “breach of the security of the system data” pursuant to the “CMS Action Plan for Notification of a Security Breach.”
3. An Agency that has a Security Policy in place and maintains a breach notification procedure that is consistent with the requirements of the Statute (815 ILCS 530/5) shall be in compliance with the requirements of this Policy.

Illinois Department of Central Management Services
DATA BREACH NOTIFICATION POLICY

REVISION HISTORY

Created: June 1, 2007
Revised: November 28, 2007
Reviewed: November 28, 2007
Effective: December 1, 2007