State of Illinois
Department of Central Management Services

IT (INFORMATION TECHNOLOGY) RECOVERY POLICY

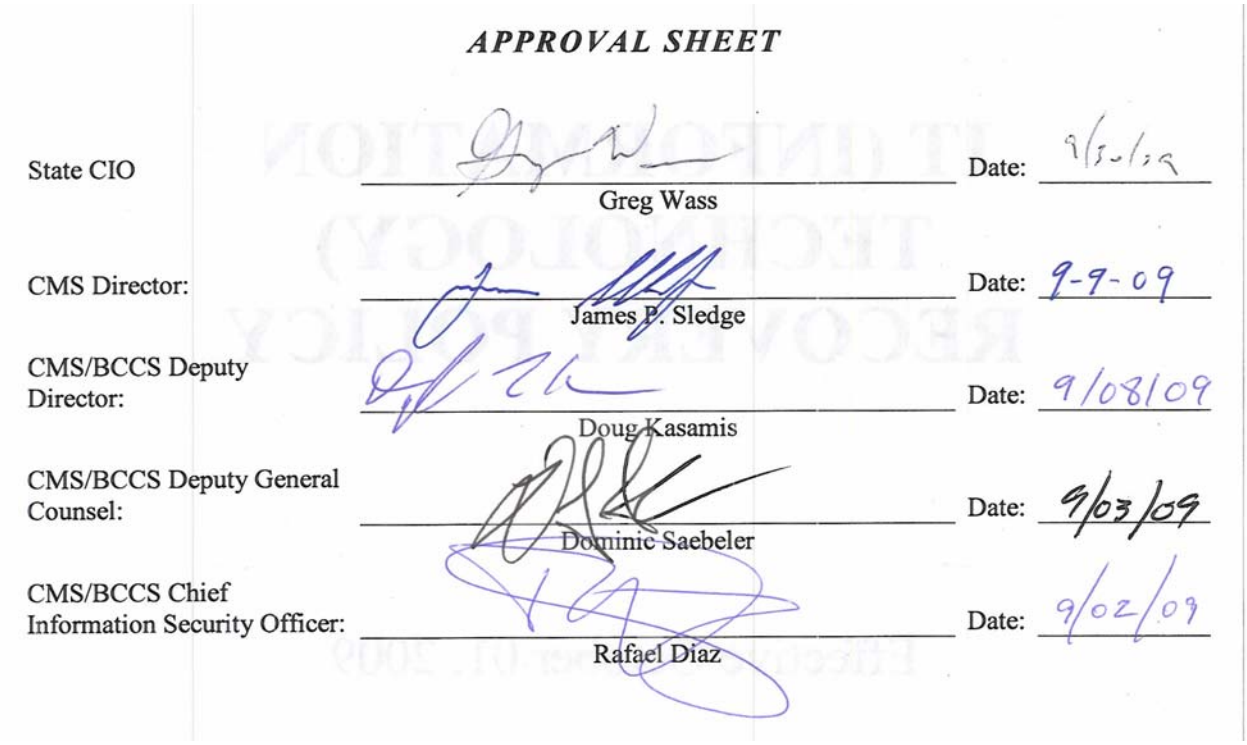
Effective October 01, 2009

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

IT (INFORMATION TECHNOLOGY) RECOVERY POLICY

Effective October 01, 2009

Version 1.0



APPROVAL SHEET

State CIO _____ Date: 9/3-1/09
Greg Wass

CMS Director: _____ Date: 9-9-09
James P. Sledge

CMS/BCCS Deputy Director: _____ Date: 9/08/09
Doug Kasamis

CMS/BCCS Deputy General Counsel: _____ Date: 9/03/09
Dominic Saebeler

CMS/BCCS Chief Information Security Officer: _____ Date: 9/02/09
Rafael Diaz

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

TABLE OF CONTENTS

POLICY STATEMENT

PURPOSE

SCOPE

DEFINITIONS

RESPONSIBILITY

POLICY

EXCEPTIONS

POLICY STATEMENT

The State of Illinois, Department of Central Management Services, Bureau of Communications and Computer Services (CMS/BCCS), in concert with supported State agencies will provide and maintain IT (Information Technology) Recovery capability designed to recover designated information systems in the event normal operation is disrupted.

PURPOSE

This policy directs the creation of supporting procedures, methods, and process documentation, and identifies the necessary roles, responsibilities, and resources that will be used to recover designated information systems hosted by CMS/BCCS.

SCOPE

The scope of this policy includes all information systems running on CMS/BCCS hosted environments.

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. **Agency Business Application** – the application and programs used by the business to process specific business functions and data associated with the application.
2. **Business Reference Model (BRM)** – the repository for capturing, cataloging and maintaining agency business application information.
3. **CMS/BCCS Hosted Environments –** a CMS/BCCS managed infrastructure used by agencies to store data and run applications.
4. **Criticality Classification** – the effect of functional failure with respect to health, safety, environment, business regularity and costs. This will determine the priority of recovery and is defined in the CMS/BCCS IT Recovery Methodology.
5. **Designated Information System** – any system identified as requiring recovery capabilities as defined in the BRM.
6. **Information System** – includes the agency business application and the CMS/BCCS hosted environment.
7. **IT Recovery Coordinator (ITRC)** – the individual(s) designated by the agency responsible for coordinating, prioritizing and directing recovery activities in their respective agency. ITRC will also coordinate recovery activities with CMS/BCCS.
8. **CMS/BCCS IT Recovery Methodology** – document for providing guidance on the following: i) business impact analysis; ii) criticality and RTO classification schema; iii) recovery procedures documentation. Details on roles and responsibilities and recovery priorities are also provided.
9. **Recovery Time Objective (RTO)** – the maximum tolerable length of time that an application can be down after a failure or disaster occurs. The RTO ranges are defined in the CMS/BCCS IT Recovery Methodology.

RESPONSIBILITY

CMS

1. CMS/BCCS is responsible for establishing procedures, methods and process documentation that designate actions, roles, and responsibilities to specific personnel to achieve policy compliance.
2. CMS/BCCS is responsible for maintaining policy and recovery methodology. Please refer to the CMS/BCCS IT Recovery Methodology for updated and detailed roles and responsibilities.

AGENCY

1. Each Agency is responsible for; developing and maintaining appropriate and viable business continuity plans, application recovery scripts, designated application information updates to the BRM, recovery exercise procedures and schedules, and on-going communications with CMS/BCCS.
2. Each Agency should also establish procedures and assign responsibility to specific agency personnel, such as an IT Recovery Coordinator to achieve policy compliance.
3. Each Agency is responsible for:
    a. understanding this policy and the CMS/BCCS IT Recovery Methodology;
    b. determining the appropriate criticality and RTO classification of their applications;
    c. communicating the criticality and RTO classification to CMS/BCCS;
    d. actively participating in local and regional exercises as business needs dictate;
    e. the cost of developing, maintaining, and exercising the recovery capabilities of their designated applications.

POLICY

1. CMS/BCCS will define and maintain the criticality classification and RTO ranges.
2. Based on agency input, CMS/BCCS collects and manages criticality classification and RTO information to provide appropriate recovery capabilities.
3. CMS/BCCS will provide the IT infrastructure for recovery of Agency designated and justified information systems.
4. CMS/BCCS will provide the IT infrastructure for recovery exercises for agency designated information systems. The agencies will schedule the exercises for their designated information systems at their own discretion.
5. CMS/BCCS will coordinate the recovery exercises for the appropriate IT infrastructure for agency designated and justified information systems and plans.
6. Agencies will provide written justification for criticality classification and RTO information to CMS/BCCS for designated information systems.
7. Agencies with designated information systems for recovery should schedule yearly local and regional exercises of their recovery plans.
8. Agencies will ensure their designated information systems have the appropriate recovery plans and recovery procedures.
9. Agencies will coordinate with CMS/BCCS to ensure their criticality classification and RTO information is current.

10. Agencies will coordinate and review with CMS/BCCS the feasibility of the recovery plans for their designated information systems.

EXCEPTIONS

1. Exceptions to this policy must be requested in writing and are granted upon verification by the CMS/BCCS Office of Security and Compliance Solutions and approval of the State CIO.
2. Mitigating controls must be identified for all exceptions granted in order to minimize the risk to the affected systems and data.