State of Illinois
Department of Central Management Services

CHANGE MANAGEMENT POLICY

Effective December 15, 2008

Revised: January 03, 2012

Version 1.2

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

CHANGE MANAGEMENT POLICY

Effective December 15, 2008
Revised January 03, 2012
Version 1.2

APPROVAL SHEET

CMS Director: Malcolm Weems Date: 2/14/12

CMS/BCCS Deputy Director: Rich Fetter Date: 2-8-12

CMS/BCCS Deputy General Counsel: Daymon Ruttenberg Date: 2.12.2012

CMS/BCCS Chief Information Security Officer: Rafael Diaz Date: 2/14/12

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

Thank You.

TABLE OF CONTENTS

POLICY STATEMENT

The Department of Central Management Services, Bureau of Communication and Computer Services (CMS/BCCS) will document all changes to the production IT infrastructure environment.

PURPOSE

This policy is to manage changes to the IT infrastructure environment in a rational and predictable manner that will help staff and customers to plan accordingly.

SCOPE

The scope includes infrastructure changes for all technology platforms and systems of the CMS/BCCS managed infrastructure and environment. All CMS/BCCS staff are responsible for implementing and maintaining changes to the CMS/BCCS managed IT infrastructure. All supported agency staff are responsible for monitoring agency processes.

DEFINITIONS

Definitions for terms used in this policy can be found in the *BCCS Terminology Glossary* located at http://bccs.illinois.gov. The term(s) and definition(s) 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. **Change** – Any alteration to the state or configuration of any production software or hardware under BCCS management and support. This would include adding new functionality, repairing or removing functionality.
2. **Change Advisory Committee (CAC)** – A group of designated individuals that represent the business entities of BCCS who meet regularly to discuss and authorize scheduled changes.
3. **Change Management** - The process of controlling modifications to hardware, software and firmware to ensure IT resources are protected against improper modification during and after system implementation.
4. **Emergency Change** – A change that does not present notification to the formal process in advance of implementation. Emergency changes will only be acceptable in the event of a system failure or the discovery of a security vulnerability to a production environment.
5. **Enterprise Change Management (ECM)** – A BCCS organizational unit responsible for overseeing all change management processes and procedures.
6. **Post Implementation Review (PIR)** - A standard method to follow up with the change owner and/or customer on the results of a change request.
7. **Production Environment** – An IT system or discrete part of an IT system (made up of hardware and system software) which is used to run software that is in live use. Also commonly referred to as a “Live Environment”. Access to the Production Environment should be restricted to authorized staff.
8. **Request for Change (RFC)** – A document that provides details on the changes proposed by the person requesting the change approval. This document is the primary input to the Change process.

9. **Scheduled Change -** Formal notification received, reviewed, and approved through the review process in advance of the change being made.
10. **System Failure –** A hardware or software failure causing the system to freeze, reboot, or stop performing its primary function. Failures which occur that can be left or maintained in an unrepaired condition until after normal business hours, and do not place the system out of service of its primary function, are not considered failures under this definition.
11. **Transparent Change –** A routine and/or minor configuration change that has no impact on system operations.

RESPONSIBILITY

It is the responsibility of all CMS/BCCS and supported agency staff to familiarize themselves with this policy and to follow all corresponding Change Management processes and/or procedures.

POLICY

1. All changes to the production IT infrastructure environment are subject to change management.
2. Emergency Changes may be implemented outside of the change management process in the event of a system failure or the discovery of a security vulnerability to a production environment.
3. All emergency changes will be reviewed and documented.
4. A CAC will meet regularly to review RFCs and ensure reviews and communications are being performed.
5. ECM will routinely review RFCs that are designated transparent to ensure criteria are being met.
6. A documented RFC must be submitted for all scheduled and emergency changes.
7. ECM may, at their discretion, deny a RFC.
8. RFCs that cause or have potential to cause outages outside pre-set authorized maintenance windows will require customer and service desk notifications.
9. Approved RFCs that are rescheduled will be subject to the approval process again.
10. A Change Management repository will be maintained for all RFCs
11. Exceptions to the Change Management Policy require authorization of the BCCS Deputy Director.