State of Illinois

Department of Central Management Services

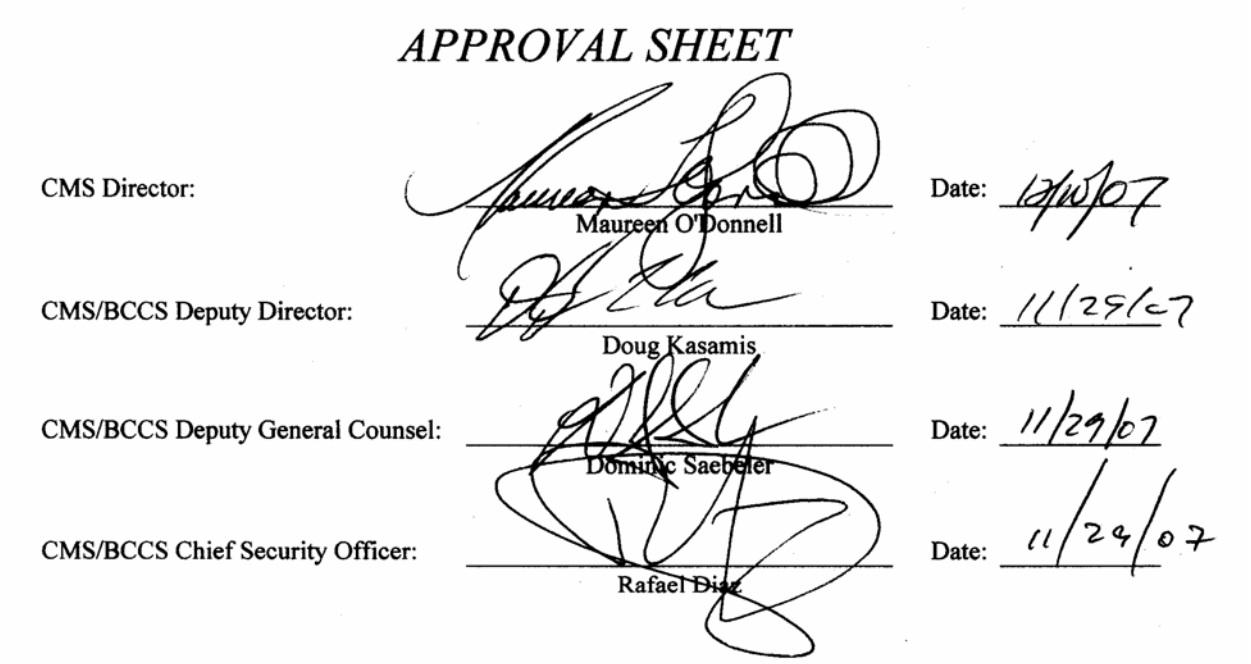
IT RESOURCE ACCESS POLICY

Effective December 1, 2007

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

IT RESOURCE ACCESS POLICY

Effective December 1, 2007
Version 1.0



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

TABLE OF CONTENTS

POLICY STATEMENT

This document focuses on granting, assigning, and revoking user access to the Illinois Department of Central Management Services (CMS), Bureau of Communication and Computer Services (BCCS) supported computer systems and networks ("Resources").

PURPOSE

This policy is designed to define what is required to manage user access to State of Illinois ("State") Resources.

SCOPE

This Policy applies to any user requiring managed access to CMS/BCCS supported computer systems.

DEFINITIONS

The following terms are used in this procedure. Additional terms may be used and can be found in the BCCS Terminology Glossary document located at the BCCS Web site bccs.illinois.gov.

1. Resource Custodian: An individual(s), identified by Agency Management, assigned responsibility for managing rules of appropriate use and protection. The State owns assets and resources purchased, acquired, and used to deliver state services. The Resource Custodians are designated and assigned the following duties including but not limited to access authorization, protection against unauthorized use, and integrity verification and revocation of access.

2. User: Any authorized person or entity assigned resource privileges by a Resource Custodian. The authozied user may use and receive a benefit from those resources the user is granted access to by the Resource Custodian.

3. Adminstrative User: Any person that has been granted special systems administrative authority to manage or maintain computer systems.

RESPONSIBILITY

1. It is the responsibility of all authorized users to understand this policy and to follow the corresponding procedures.

2. All Resource Custodians are responsible for understanding and adhering to this Policy and for granting, reviewing, and removing access to resources that have been assigned to them to protect.

3. CMS and client agency security personnel, or their designee, are responsible for monitoring, auditing, tracking, and validating compliance with policies and procedures and conducting investigations into violations of law, policies, or procedures.

4. CMS and Shared Services Human Resources personnel are responsible for ensuring that appropriate identity verification and background checks are performed for all staff and contractors requiring access to BCCS-supported Resources.

POLICY

1. Identity must be validated prior to the granting of authority to access a protected State resource.

2. Access to IT resources will be allocated based on justified business need.

3. IT resources must be used for approved use only. Approved use is limited to authorized users, sanctioned State business, job responsibility, and reasonable personal use.

4. A security screening review (background check) may be conducted on any individual requesting access to any State resource (physical or logical). Access may be delayed until the review is completed. Access may be denied based on impartial analysis of facts uncovered by the review.

5. No expectation of privacy exists when a State resource is accessed or used. That is, authorized personnel may review, filter, monitor, track, audit, or otherwise view any resource and/or activity including but not limited to e-mail, Internet, private disk drives, office furniture, etc.

6. All knowledge and information derived or acquired through access to State resources or from access to State premises, respecting secret, confidential, or proprietary matters of the State, shall for all time and for all purposes be regarded as strictly confidential and be held in trust and solely for State of Illinois benefit and use and shall not be directly or indirectly disclosed to any person other than authorized personnel without appropriate written permission.

7. Each individual needing access to a CMS protected IT resource may be issued a physical badge, and/or digital certificate, and/or User ID in order to validate identity.

8. Administrative User access must be approved by an appropriate section manager responsible for managing a particular system(s).

9. Upon separation, Administrative User access rights and authorization will be disabled by changing the password or access token of any system(s) to which the Administrative User had access.

10. Access will be revoked when a user is no longer authorized; examples include separation, discipline or change of business need. It is the responsibility of the data custodian and/or Employee Manager to submit these revocation requests.

11. Access can be revoked at the discretion of the Resource Custodian, employee manager, or other authorized personnel.

REVISION HISTORY

Created:	June 1, 2007
Revised:	October 16, 2007
Reviewed:	October 16, 2007
Effective:	December 1, 2007