State of Illinois
Department of Central Management Services

GENERAL SECURITY FOR STATEWIDE IT RESOURCES POLICY

Effective December 15, 2008

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

GENERAL SECURITY FOR STATEWIDE IT RESOURCES POLICY

Effective December 15, 2008
Version 1.2

Revised January 1, 2010

APPROVAL SHEET

CMS Director: James P. Sledge Date: 12-23-09

CMS/BCCS Deputy Director: Rich Fetter Date: 12-23-09

CMS/BCCS Deputy General Counsel: Dominic Saebeler Date: 12-23-09

CMS/BCCS Chief Information Security Officer: Rafael Diaz Date: 12/22/09

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

Thank You.

Illinois Department of Central Management Services

General Security

For Statewide IT Resources Policy

TABLE OF CONTENTS

Illinois Department of Central Management Services

General Security
For Statewide IT Resources Policy

POLICY STATEMENT

The Department of Central Management Services, Bureau of Communication and Computer Services (CMS/BCCS) will provide security for CMS/BCCS managed IT resources to ensure the confidentiality, integrity and availability of State of Illinois operations.

PURPOSE

This policy defines responsibilities and general security measures specific to the use of information technology (IT) resources managed by CMS/BCCS.

SCOPE

This policy applies to all State of Illinois governmental agencies, boards and commissions that connect to the CMS/BCCS managed network resources.

DEFINITIONS

Definitions for terms used in this policy can be found in the *BCCS Terminology Glossary* located at http://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. **Administrative User:** Any person that has been granted special systems administrative authority to manage or maintain computer systems.
2. **IT Resources** are categorized as follows: Physical, Logical, and Communications. Physical resources include but are not limited to desktop computers, portable computers, personal information devices, and printers. Logical resources include computer software and data files digitally or optically stored as well as information itself. Communication resources include the capability to send messages either through the State internal network or via the Internet.
3. **Resource Custodian:** An individual 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.
4. **User:** any authorized person or entity assigned resource privileges by a Resource Custodian to administer, manage, develop or maintain an IT resource for State operations.

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. It is the responsibility of all authorized users of IT Resources to understand and adhere to this Policy.
3. All Resource Custodians are responsible for understanding and adhering to this policy.
4. Statewide 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.

5. It is the responsibility of State-wide IT staff to inform CMS/BCCS, in writing, of any special Use requirements outside of this policy.
6. Managers and supervisors are also responsible for resource inventory, for documenting access rights and resource allocation; and for ensuring that all State resources (equipment, devices, keys, badges, access cards, etc.) are returned when the user is no longer performing work for the State of Illinois.

POLICY

1. RESOURCE USE - GENERAL PROVISIONS

a. IT Items purchased by the State, regardless of funding source, are owned by the State. Other sources of acquisition may also result in the State owning an IT resource. These include but are not limited to donations or transfers from one state entity to another.

b. Identity must be validated prior to the use of a protected IT resource.

c. 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.

d. Where appropriate, data and information classification guidelines will be developed and published to assist Resource Custodians in determining the level of control applied to IT Resource use.

e. No IT resource shall be used to communicate, generate, or store information which is illegal or may be considered offensive, harassing, threatening, intimidating, violent, sexually explicit, racially / ethnically offensive, or otherwise considered contributing to a hostile work environment.

f. Use of IT resources may be filtered, monitored, suspended, or terminated at the discretion of the Resource Custodian or designee, or Law Enforcement based on approved criteria including but not limited to job duty changes, access inactivity, security concerns, policy violation(s), or other events deemed appropriate by the Resource Custodian.

g. Reasonable action, due care, and due diligence must be taken to prevent inappropriate use, disclosure, destruction, or theft of State IT Resources. Reasonable actions include but are not limited to preventive, detective, and corrective measures such as encryption, anti-viral software, and application of security patches.

h. Proper disposal methods, as detailed in corresponding operational procedures, must be applied to any IT resource containing or storing potentially confidential or sensitive information.

i. Appropriate designated personnel are assigned the responsibility and authority to access, audit, review, filter, monitor, trace, intercept, recover, block, revoke, restrict, delete, or disclose (within policy and procedural limitations) any action, data, or behavior involving a State IT Resource.

j. 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 of the Resource Custodian.

k. All forms of communication using a State resource may be monitored or recorded without the consent or knowledge of the sendor or receiver.

l. Disclosure of information classified as confidential or sensitive is restricted to only authorized parties and in a manner consistent with the form of data classification.

m. Only approved software and hardware are authorized to be loaded on State resources:

   i. Users are not authorized to run software that has not been approved by CMS/BCCS technical staff.

   ii. Users are not authorized to attach hardware not approved by CMS/BCCS technical staff including but not limited to modems or non-State devices such as portable computers or other digital storage or writing devices.

   iii. Only approved software may be used to develop applications or to manipulate data;

n. Business decisions should not be made based on user developed applications unless that application has been verified as accurate and maintains minimum security controls and data integrity standards and controls;

2. RETURN AND DISPOSAL

a. Once the business need that justified allocation of the IT resource is no longer valid, the user must return the IT resource or notify appropriate parties that access is no longer needed.

b. When a user separates from State employment or ends a contractual obligation, all State IT resources must be returned.

c. When an IT resource is moved or re-assigned, appropriate inventory actions must be performed to ensure Agency inventory controls are up to date.

d. Once an IT resource exceeds its usefulness, such as outdated or end-of-life computer equipment or malfunctioning data cartridges, the resource must be disposed of or recycled in a proper manner.

3. SECURITY AWARENESS

a. New employees are required to participate in employee orientation to include certifying that they have completed any required security awareness training and agree to comply with this General Security for Statewide IT Resources.

b. Current employees shall, at each annual performance evaluation, certify that they have completed any required security awareness training and agree to comply with this General Security for Statewide IT Resources.

c. Supervisors are responsible for ensuring that each employee has completed appropriate security awareness training and has documented it in the employee’s personnel file.

4. CREDENTIALS / LOGIN RULES

a. Details of user identification (UID) best practices can be found in the latest version of the “BCCS IT Resource Access Policy” found at http://bccs.illinois.gov.

b. Details of password establishment and use requirements can be found in the latest version of the “BCCS Credential Standard”.

5. INAPPROPRIATE ACTIVITIES

Specific actions which are prohibited; include but are not limited to:

a. Illegal activities;

b. Copyright violations (text, video, digital image, audio, music, or other media) and/or breaches of license agreement;

c. Violatations of the Illinois Ethics Act;

d. Harassment or intimidation (sexual, religious, ethnic, etc.);

e. Libelous, slanderous, degrading, insulting, vulgar, obscene, offensive, or hostile remarks, and/or emails, and/or websites;

f. Utilizing State resources in pursuit of one’s personal business;

g. Unauthorized downloading including but not limited to downloading of music (unless specific to an assigned job duty), offensive images (pornography, hate, etc.), political or campaign data that violates ethics or campaign reform legislation, or any other deliberate action that violates the intent of a State policy, procedure, or standard;

h. The use of unauthorized or illegal peer to peer software programs on state owned computers.

i. Deliberate and premeditated actions that degrade delivery of service of any IT resource or resulting client deliverable and/or the introduction of a virus, Trojan horse, malware, spyware, key-capture software, or other unauthorized software that may pose a risk to normal operation of an IT resource or delivery of a service;

j. Access to another user’s IT resource without specific and direct authorization and based on a business need for access;

k. Violation of confidential and/or proprietary safeguards that place the State or individuals at risk of legal action or that could cause embarrassment to the State or an individual;

l. Participation in any activity that could potentially cause damage to the image of the State, an agency, or an individual State worker including but not limited to online auctions, personal shopping, private/personal chat room conversations, etc.;

m. Any action that would cause a detriment to the image, character, reputation, or public confidence of State operations;

n. Sending confidential information in an unsecured e-mail, unencrypted through the Internet;

o. Discussing confidential information verbally in a public place or within hearing distance of unauthorized individuals.

6. COMPUTER LOCKING / SCREEN SAVERS

a. Password protected Locking / Screen Saver technology should be employed by the Resource Custodian to ensure confidential / private information is secure and protected.

b. Before leaving the desktop / laptop unattended the screen saver should be engaged to lock the device.

7. INCIDENT REPORTING

a. All actual or suspected instances of information asset misuse, theft or abuse, as well as potential threats (e.g., hackers, computer viruses) or obvious weaknesses affecting security, must be reported to your immediate supervisor.

b. All serious infractions including, but not limited to, pornography or violence, must be immediately reported to your immediate supervisor.

c. Any actual or suspected security breach, including any lost or broken IT resource asset must be immediately reported to your immediate supervisor.

8. E-MAIL

a. All broadcast messages to all Users within a given post office must be reviewed and approved by authorized agency management or their legal department.

b. All email disclaimers must be approved by agency management.

c. Recipients of messages or information inadvertently sent or misaddressed to them should not copy, retain or disclose the contents of such messages. Such messages shall be deleted and the sender shall be notified, if possible, that the message was misaddressed or misdirected.

d. All email related data should be stored on a network drive.

e. Upon separation, the User will no longer have access to their email account or data associated with that account.

9. EXCEPTIONS

a. Exceptions to this policy must be requested in writing and are granted upon verification by the CMS/BCCS Office of Security and Compliance Solutions. Requests will be processed through the existing Enterprise Service Requests (ESR) process.

b. Mitigating controls must be identified for all exceptions granted in order to minimize the risk to the affected systems and data.