State of Illinois
Department of Central Management Services

GENERAL SECURITY FOR STATEWIDE NETWORK RESOURCES POLICY

Effective December 15, 2008

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

GENERAL SECURITY FOR STATEWIDE NETWORK RESOURCES POLICY

Effective December 15, 2008

Version 1.1

Revised January 01, 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 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 provide security for CMS/BCCS managed network 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 network 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://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 this policy, the definition below shall control for this Policy.

1. **Access Point (AP)** – A hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired LAN.
2. **Broadband -** high-speed Internet access—typically contrasted with dial-up access over a modem.
3. **Citrix -** is a remote access/application publishing product that allows people to remotely connect to applications available from central servers.
4. **CMS Wireless Zone** – A CMS-controlled and authorized wireless hot spot that is made available for access to the Internet and CMS resources. Anyone with a wireless router is creating a wireless zone (hot spot).
5. **Content Filtering -** the use of a program to screen and exclude from access or availability Web pages or e-mail that is deemed objectionable.
6. **DSL -** (Digital Subscriber Line) - a technology for bringing high-bandwidth information to homes and small businesses over ordinary copper telephone lines.
7. **Firewall -** a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks
8. **Hotspot** – A place within a wireless zone that contains a high concentration of wireless access points and/or routers.
9. **IDS/IPS -** a system that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).
10. **Remote access -** connectivity hardware and software including but not limited to: VPN, modem, Citrix, telnet, FTP, and EDI.

11. **Telnet -** Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers. Through Telnet, an administrator or another user can access someone else's computer remotely.
12. **VPN -** A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.
13. **Vulnerability Assessments -** A security audit that systematically evaluates the security of an organization's information system by measuring how well it conforms to a set of established criteria.
14. **Wireless data communication devices** – include personal computers, laptops, routers, and network interface cards connected to any CMS Wireless Zone.
15. **Wireless Service** – The provision of wireless computing capabilities within a wireless zone.
16. **Off-Net Services** – Alternate wide area network and internet services not managed nor supported by CMS/BCCS. These include, but are not limited to: City-wide or municipality wide wireless networks, DSL, or Broadband Cable (High Speed Cable Internet).

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 CMS/BCCS managed network resources to understand and adhere to this Policy.
3. All Resource Custodians are responsible for understanding and adhering to this policy.
4. 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 Agency staff to inform BCCS, in writing, of any exceptions or 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.
7. CMS/BCCS is responsible for the maintenance, support and security of the Infrastructure and resources established to provide services for the network.

POLICY

Firewall / Intrusion Detection & Prevention

1. It is a violation of policy for anyone to attempt to bypass, to penetrate, to alter the configuration of, or to otherwise affect the operation of any CMS/BCCS managed firewall, router, intrusion detection / prevention device or other network infrastructure device unless they are an authorized CMS/BCCS staff member.
2. All IDS/IPS implementations in the CMS/BCCS managed network must be approved by CMS/BCCS. Any unauthorized or rogue IDS/IPS devices found in the CMS/BCCS managed network will be removed.

Wireless LAN

1. Central Management Services (CMS), Bureau of Communication and Computer Services (BCCS) will centrally manage the acquisition, installation, operations, and maintenance of wireless Access Points (APs) in the CMS Wireless Zone.
2. All wireless APs connected to the CMS/BCCS network must be registered through CMS/BCCS LAN Services APs will be scanned by CMS/BCCS Information Security for vulnerabilities to assess the defined base level of security relevant to the network.
3. Access points/wireless zones will be periodically screened for unauthorized or rogue access points, stations, and bridges.
4. Client wireless data communication devices accessing the CMS Wireless Zone must follow all the same guidelines for access to the network as for the wired Local Area Network (LAN) including network registration, antivirus software, up-to-date patches, and strong credentials that comply with CMS/BCCS Credential Standards.
5. All CMS/BCCS wireless APs must comply with the CMS/BCCS Encryption Standard.

Content Filtering

1. CMS/BCCS is responsible for implementing and maintaining the CMS Web content filtering system.
2. It is a violation of policy for anyone to attempt to bypass, to penetrate, to alter the configuration of, or to otherwise affect the operation of any CMS/BCCS managed filtering system unless they are an authorized CMS/BCCS staff of Network Services.

Vulnerability Assessments

1. CMS/BCCS reserves the right to perform vulnerability assessments and network scans as necessary to ensure the security and availability of the environment.
2. When requested, and for the purpose of performing an audit, consent to needed access will be provided to members of the CMS/BCCS staff.
3. Agencies hereby provide their consent to allow the CMS/BCCS staff to access the agency’s networks and/or firewalls to the extent necessary to perform the scans with access as outlined in this policy.

   This access may include:

   a. User level and/or system level access to any computing or communications device
   b. Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on State of Illinois equipment or premises
   c. Access to work areas (labs, offices, cubicles, storage areas, etc.)
   d. Access to interactively monitor and log traffic on CMS/BCCS managed networks.
4. Agencies shall provide protocols, addressing information, and network connections sufficient for CMS/BCCS staff to utilize the software to perform network scanning.
5. No one outside of CMS/BCCS staff may perform vulnerability scanning on the CMS/BCCS managed network without written permission from CMS/BCCS.

Remote Access

1. Remote access gateways will be set up, configured and managed by CMS/BCCS.
2. Only CMS/BCCS authorized and configured remote access clients may be used.
3. All computers with remote access connectivity to CMS/BCCS managed internal networks must use the most up-to-date approved anti-virus software.

4. All computers with remote access connectivity to CMS/BCCS managed internal networks must have the latest security patches applied.
5. Computers that are not state-owned equipment or in an untrusted network must be approved by CMS/BCCS network staff before equipment is brought online.
6. Personal equipment using remote access connectivity is a de facto extension of CMS/BCCS managed network, and as such are subject to CMS/BCCS policies. Remote access client software must be removed from personal equipment once no longer connected to state resources.
7. Only approved remote access hardware and software will be allowed access to the network for specific justified business needs when other more secure means are not available.
8. All approved remote access hardware and software will require standard security measures for authentication, access and software.

Wide-Area Network (WAN), Internet Services, Off-Net Services

1. State Agencies are required to request all Wide-Area Network and Internet Services through CMS BCCS.
2. Off-Net service will be approved for use by State of Illinois Agencies based approvals by CMS/BCCS network staff.
3. All computers with Off-Net service connectivity to CMS/BCCS managed internal networks must use the most up-to-date anti-virus software.
4. All computers with Off-Net service connectivity to CMS/BCCS managed internal networks must have the latest security patches applied.
5. There will be no responsibilities, written or understood, associated with CMS/BCCS and any applications that obtain service through Off-Net connections.
6. Outages related to facilities that are not under the control of CMS/BCCS are the responsibility of the controlling Agency.
7. If the building has existing State Data Network Connectivity, an additional exception must be approved by CMS/BCCS.

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. Requests will be processed through the existing Enterprise Service Requests (ESR) process.
2. Mitigating controls must be identified for all exceptions granted in order to minimize the risk to the affected systems and data.