Illinois Department of Human Services

Cornerstone System Security Plan

November, 2012

Version - Final

Document Created by: Illinois WIC

Name	Title
Penny Roth	DHS, CHP, Chief: Bureau of Family Nutrition
Steve Strode	DHS, CHP, Assistant Chief: Bureau of Family Nutrition
Stephanie Bess	DHS, CHP, Program Coordinator: Bureau of Family Nutrition
Joanne Durkee	DHS, CHP, Bureau Chief: Performance Support Services
AnnMarie Anderson	DHS, MIS, Business Analyst
Eric Fyalka	DHS, MIS, Business Analyst
Hal Waggoner	DHS, MIS, Section Manager: Cornerstone and UHS
Julie Hagele	DHS, MIS, Assistant CIO/Security

Document Revision History

Activity	Version	Date
Reviewed by internal group – analysts turned the doc back over to division staff for next iteration.	draft	12-9-2011
DHS revised the document pursuant to FNS's original comments referenced in 02-03-2012 email.	draft	03-15-2012
Added Biennial Review information – section 2.1.1	draft	04-30-2012
Added Physical Control data – section 2.2	draft	07-20-2012
Approved by USDA	Final	11-2012

Table of Contents

Attachments

Attachment A - The IT Recovery Methodology

1 General Information

The Illinois WIC Program is supported by Cornerstone, Illinois' maternal and child health management information system (MIS). The purpose of this document is to summarize the security requirements for the agency business application, Cornerstone, and the CMS/BCCS hosted environment for Cornerstone; and describes the security controls in place or planned for meeting those requirements. Management information systems (MIS) that are used to capture, create, store, process or distribute classified information must be properly managed to protect against unauthorized disclosure of classified information, loss of data integrity, and to ensure the availability of the data and system. Protection requires a balanced approach including IS security features to include but not limited to, administrative, operational, physical, computer, communications, and personnel controls. Protective measures commensurate with the classification of the information, the threat, and the operational requirements associated with the environment of the MIS are required. The requirements outlined in the following sections apply to all information systems processing classified information.

2 WIC Policy – Management Information Systems Effective: 2012

The Management Information System (MIS) for the Illinois WIC Program is Cornerstone. All WIC staff must follow the Cornerstone User Manual expectations for entering and utilizing data to ensure proper service delivery. Staff must be trained on system security and observe appropriate separation of duties within the system as defined below per the USDA Handbook 901.

2.1 Security Awareness, Training, and Education

Staff who manage, program, operate, maintain, or use Cornerstone should be aware of their security responsibilities.

- Security training must be provided before system users are allowed access to the system.
- Security training is designed to help system users become familiar with using Cornerstone's security features. Security training also ensures that users understand their responsibilities and security procedures for protecting any sensitive information they manage. Security training includes:
    - The importance of protecting client privacy and data confidentiality.
    - How to identify a security incident.

2.1.1 Security Reviews

IL WIC will regularly, and no less than biennially, review the MIS security of installations involved in the administration of FNS programs according to State security policy. At a minimum, the reviews shall evaluate physical and data security, operating procedures, and personnel practices. IL WIC will provide a written summary of review findings and

determination of compliance with requirements to FNS upon request or at least biennially after completion of the Management Information System Security Review. IL WIC will include an action plan with scheduled dates of milestones which, when completed, will correct any security weaknesses.

- Periodic refresher (e.g., annual) security training is required for continued access to the system.
- Security Reviews will be conducted that administer FNS programs at least biennially and make the results of this review available to FNS. The reviews are designed to ensure the following:
    - Sufficient controls and security measures are in place to compensate for any identified risks associated with the program/system and/or its environment.
    - The program/system is being operated cost-effectively and complies with applicable laws and regulations.
    - Program/systems' information is properly managed.
    - The program/system complies with management, financial, information technology (IT), accounting, budget, and other appropriate standards.

2.2 Technical Controls

Technical controls focus on both functional and physical controls established to prevent fraud.

- **Separation of duties** - is defined as assigning key duties to individuals, such as enrolling a new participant, entering required health information, generating risk factors or issuing food instruments.
    - Staff members must not have "full access" to the following screens beyond a "View Only" capacity without annual approval from the state.
        - Participant Enrollment
        - Medical Screens
        - WIC Assessment
        - Produce Food Instruments
- **Physical Controls** - are measures designed to prevent unauthorized physical access to equipment, facilities, material, information, and documents. Physical resources include but are not limited to desktop computers, portable computers, personal information devices, and printers. Rooms containing system hardware and software such as local area network rooms or telephone closets should be secured to ensure that they are accessible to authorized personnel only. Safeguards should be in place to protect check and voucher stock.
    - The Agency "Service Level Agreements/Contract" document identifies specific guidance local agencies must follow to address physical security.

3 Management Controls

Protection of information assets and maintaining the confidentiality, integrity and availability of DHS Cornerstone information technology assets and telecommunications resources are vital in meeting the Illinois WIC Program's delivery requirements. Implementation of security measures such as a risk management program, effective security controls, certification and accreditation of IT systems and updated security plans are vital components in this plan.

3.1 General Security for Statewide Network Resources Policy

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.

3.1.1 Purpose

This policy defines responsibilities and general security measures specific to the use of network resources managed by CMS/BCCS.

3.1.2 Scope

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

3.1.3 Responsibility

- 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.
- It is the responsibility of all authorized users of CMS/BCCS managed network resources to understand and adhere to this Policy.
- All Resource Custodians are responsible for understanding and adhering to this policy.
- 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.
- It is the responsibility of Agency staff to inform BCCS, in writing, of any exceptions or special Use requirements outside of this policy.
- 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.
- CMS/BCCS is responsible for the maintenance, support and security of the Infrastructure and resources established to provide services for the network.

3.1.4 Firewall / Intrusion Detection & Prevention

- 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.
- 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.

3.1.5 Wireless LAN

- 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.
- 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.
- Access points/wireless zones will be periodically screened for unauthorized or rogue access points, stations, and bridges.
- 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.
- All CMS/BCCS wireless APs must comply with the CMS/BCCS Encryption Standard.

3.1.6 Content Filtering

- CMS/BCCS is responsible for implementing and maintaining the CMS Web content filtering system.
- 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.

3.1.7 Vulnerability Assessments

- CMS/BCCS reserves the right to perform vulnerability assessments and network scans as necessary to ensure the security and availability of the environment.
- When requested, and for the purpose of performing an audit, consent to needed access will be provided to members of the CMS/BCCS staff.
- 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:
    - User level and/or system level access to any computing or communications device
    - Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on State of Illinois equipment or premises
    - Access to work areas (labs, offices, cubicles, storage areas, etc.)
    - Access to interactively monitor and log traffic on CMS/BCCS managed networks.
- Agencies shall provide protocols, addressing information, and network connections sufficient for CMS/BCCS staff to utilize the software to perform network scanning.
- No one outside of CMS/BCCS staff may perform vulnerability scanning on the CMS/BCCS managed network without written permission from CMS/BCCS.

3.1.8 Remote Access

- Remote access gateways will be set up, configured and managed by CMS/BCCS.
- Only CMS/BCCS authorized and configured remote access clients may be used.
- All computers with remote access connectivity to CMS/BCCS managed internal networks must use the most up-to-date approved anti-virus software.
- All computers with remote access connectivity to CMS/BCCS managed internal networks must have the latest security patches applied.
- 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.
- 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.
- 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.
- All approved remote access hardware and software will require standard security measures for authentication, access and software.

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

- State Agencies are required to request all Wide-Area Network and Internet Services through CMS BCCS.
- Off-Net service will be approved for use by State of Illinois Agencies based approvals by CMS/BCCS network staff.

- All computers with Off-Net service connectivity to CMS/BCCS managed internal networks must use the most up-to-date anti-virus software.
- All computers with Off-Net service connectivity to CMS/BCCS managed internal networks must have the latest security patches applied.
- There will be no responsibilities, written or understood, associated with CMS/BCCS and any applications that obtain service through Off-Net connections.
- Outages related to facilities that are not under the control of CMS/BCCS are the responsibility of the controlling Agency.
- If the building has existing State Data Network Connectivity, an additional exception must be approved by CMS/BCCS.

3.2 Data Classification and Protection

The State of Illinois, Department of Central Management Services, Bureau of Communications and Computer Services (CMS/BCCS) will maintain a data classification and protection schema designed to enable the protection of data from unauthorized disclosure, use, modification, or deletion. The determinations to be made in accordance with this policy are subject to the requirements of state or federal law, rules, or regulations.

3.2.1 Purpose

The purpose of this policy is to inform State of Illinois data owners and data users about the data classification and protection schema used by CMS/BCCS for protecting data generated, accessed, transmitted and stored by State of Illinois resources; and to promote compliance with local, state, and federal regulations regarding privacy and confidentiality.

3.2.2 Scope

This data classification policy is applicable to all structured and unstructured data generated, accessed, transmitted or stored on systems and networks managed by CMS/BCCS.

3.2.3 Responsibility

- In order to implement this policy, CMS may establish procedures and assign responsibility to specific personnel. Each Agency may also establish procedures and assign responsibility to specific agency personnel to achieve policy compliance.
- The Data Owner is responsible for:
    - Determining the appropriate classification (as defined below) of information generated by the owner or agency.
    - Communicating the information classification when the information is released outside of the agency or the State of Illinois.
    - Communicating the information classification to CMS/BCCS and the Resource Custodian so that they may provide the appropriate levels of protection.

- Data Owners and Data Users are responsible for using structured and unstructured data in compliance with this policy.
- The Data Owner is responsible for ensuring the appropriate security and protection protocols are in place.
- CMS/BCCS is responsible for the overall security of the CMS/BCCS managed hosting environment.
- It is an affirmative obligation of each individual to report violations of this policy to their supervisors or agency executives.

3.2.4 Policy

- CMS/BCCS classifies data into one of the following three categories:
    - Public
    - Official Use Only
    - Confidential
- All data must be adequately protected based on the existing statutory regulations and the applicable industry principles – e.g., HIPAA, PCI, FTI, and PII – as defined by the Data and System Owners, in concert with CMS/BCCS.
- Agencies must classify each information technology ("IT") system by category according to the most confidential data that the IT system stores, processes, or transmits.
- All Data must be retained and destroyed in accordance with the State Records Act.

3.2.5 Schema

- **PUBLIC DATA -** Public Data is information that may or must be open to the general public. It is defined as information with no existing local, state, national or international legal restrictions on access or usage. Public data, while subject to State of Illinois disclosure rules, is available to all residents of the State of Illinois and to all individuals and entities external to the State of Illinois.
- **OFFICIAL USE ONLY DATA -** Official Use Only Data is information that must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Official Use Only Data is information that is restricted to certain employees of the State of Illinois who have a legitimate purpose for accessing such data. Data Owners may designate data as Official Use Only.
- **CONFIDENTIAL DATA -** Confidential Data is information protected by statutes, regulations, State of Illinois policies, or contractual language. Disclosure to parties outside the State of Illinois should be authorized by executive management and/or the Data Owners and General Counsel. Disclosure of Confidential Data internal to the State

of Illinois should be on a need-to-know basis only. Confidential data includes any data of which the inappropriate disclosure could have a material adverse effect on State of Illinois interests, the conduct of agency programs, or the privacy to which individuals are entitled.

3.3 IT Resource Access policy

This section 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").

3.3.1 Purpose

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

3.3.2 Scope

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

3.3.3 Responsibility

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

3.3.4 Policy

- Identity must be validated prior to the granting of authority to access a protected State resource.
- Access to IT resources will be allocated based on justified business need.
- 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.
- 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.

- 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.
- 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.
- 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.
- Administrative User access must be approved by an appropriate section manager responsible for managing a particular system(s).
- 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.
- 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.
- Access can be revoked at the discretion of the Resource Custodian, employee manager, or other authorized personnel.

3.4 Statewide CMS/BCCS Facility Access Policy

The Department of Central Management Services, Bureau of Property Management CMS/BoPM administers the granting, assigning, and revoking of physical access privileges to CMS/BCCS statewide computing facilities.

3.4.1 Purpose

This policy defines the requirements for granting and revoking an individual's physical access privileges to these facilities.

3.4.2 Scope

This policy applies to any individual requiring physical access privileges to a CMS/BCCS facility located anywhere in Illinois.

3.4.3 Responsibility

- 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.

- It is the responsibility of any individual requiring physical access privileges to CMS/BCCS facilities, to understand this policy and follow the corresponding procedures.
- CMS/BCCS 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 this policy and any associated procedures.

3.4.4 Policy

- Identity must be validated prior to the granting of physical access privileges.
- Physical access to CMS/BCCS facilities will be assigned based on justified and documented business need and approved use only. Approved use is limited to an authorized individual's job responsibilities and sanctioned State business.
- A security screening review (background check) will be conducted on any individual requesting unescorted physical access to CMS/BCCS facilities. Access will be delayed until the review is completed. Access may be denied based on impartial analysis of facts uncovered by the review.
- An individual requesting physical access to a CMS/BCCS facility MUST produce valid identification to be considered for initial issuance of a credential. Anyone appearing to obtain a new credential MUST have the identification on hand, or they will be turned away without a new credential.
- Unauthorized individuals requesting physical access to a CMS/BCCS facility must follow the defined procedures for escorted access.
- Each individual granted physical access will be issued a credential. The credential must be prominently displayed. The credential must be used to enter and exit CMS/BCCS facilities.
- CMS/BCCS reserves the right to perform an updated background check on all authorized individuals.
- Individuals granted escorted physical access privileges must return credentials upon exiting a CMS/BCCS facility. It is the responsibility of the escort or the facility security personnel to ensure the recovery of credentials.
- Physical access privileges will be revoked, and credentials will be recovered, when an individual is no longer authorized; examples include separation, discipline or change of business need. It is the responsibility of the Resource Custodian and/or Employee Manager to submit these revocation requests and ensure the recovery of the credentials.
- Physical access privileges, escorted or unescorted, can be revoked at any time at the discretion of the Resource Custodian, employee manager, or other authorized personnel.

4 Operational Controls

This area focuses on addressing security methods on mechanisms primarily implemented and executed by peopled (as opposed to systems). These controls are put in place to improve the security of a system.

4.1 General Security for Statewide IT Resources Policy

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.

4.1.1 Purpose

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

4.1.2 Scope

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

4.1.3 Responsibility

- 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.
- It is the responsibility of all authorized users of IT Resources to understand and adhere to this Policy.
- All Resource Custodians are responsible for understanding and adhering to this policy.
- 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.
- It is the responsibility of State-wide IT staff to inform CMS/BCCS, in writing, of any special Use requirements outside of this policy.
- 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.

4.1.4 Resource Use – General Provisions

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

- 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.
- 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.
- 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.
- 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.
- 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.
- Proper disposal methods, as detailed in corresponding operational procedures, must be applied to any IT resource containing or storing potentially confidential or sensitive information.
- 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.
- 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.
- All forms of communication using a State resource may be monitored or recorded without the consent or knowledge of the sender or receiver.
- 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.
- Only approved software and hardware are authorized to be loaded on State resources:
    - Users are not authorized to run software that has not been approved by CMS/BCCS technical staff.

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

- 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.

4.1.5 Return and Disposal

- 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.
- When a user separates from State employment or ends a contractual obligation, all State IT resources must be returned.
- When an IT resource is moved or re-assigned, appropriate inventory actions must be performed to ensure Agency inventory controls are up to date.
- 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.

4.1.6 Security Awareness

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

4.1.7 Credentials/Login Rules

- 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.
- Details of password establishment and use requirements can be found in the latest version of the "BCCS Credential Standard".

4.1.8 Inappropriate Activities

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

- Illegal activities;
- Copyright violations (text, video, digital image, audio, music, or other media) and/or breaches of license agreement;
- Violations of the Illinois Ethics Act;
- Harassment or intimidation (sexual, religious, ethnic, etc.);
- Libelous, slanderous, degrading, insulting, vulgar, obscene, offensive, or hostile remarks, and/or emails, and/or websites;
- Utilizing State resources in pursuit of one's personal business;
- 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;
- The use of unauthorized or illegal peer to peer software programs on state owned computers.
- 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;
- Access to another user's IT resource without specific and direct authorization and based on a business need for access;
- 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;
- 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.;
- Any action that would cause a detriment to the image, character, reputation, or public confidence of State operations;
- Sending confidential information in an unsecured e-mail, unencrypted through the Internet;
- Discussing confidential information verbally in a public place or within hearing distance of unauthorized individuals.

4.1.9 Computer Locking/Screen Savers

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

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

4.1.10 Incident Reporting

- 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.
- All serious infractions including, but not limited to, pornography or violence, must be immediately reported to your immediate supervisor.
- Any actual or suspected security breach, including any lost or broken IT resource asset must be immediately reported to your immediate supervisor.

4.1.11 E-mail

- All broadcast messages to all Users within a given post office must be reviewed and approved by authorized agency management or their legal department.
- All email disclaimers must be approved by agency management.
- 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.
- All email related data should be stored on a network drive.
- Upon separation, the User will no longer have access to their email account or data associated with that account.

4.2 Back up Retention Policy

The Department of Central Management Services (CMS) Bureau of Communications and Computer Services (BCCS) will back up electronically stored information (ESI) to promote the restoration of service in the event of failure resulting from a disaster.

4.2.1 Purpose

The purpose of this policy is to define the backup/recovery policy for information technology (IT) systems owned and operated by CMS BCCS. This policy is designed to protect State of Illinois ESI, thus ensuring ESI is not lost and can be recovered in the event of a disaster.

4.2.2 Scope

This policy applies to all ESI used and stored on the IT systems owned and operated by CMS BCCS.

4.2.3 Responsibility

- It is the responsibility of CMS to establish standards for the backup or restoration of ESI.

- It is the responsibility of each Agency to identify any unique requirements for backup or restoration of ESI in the event of failure.

4.2.4 Policy

- Each IT system will be backed up according to its unique characteristics and requirements.
- Specific back up procedures, standards, and requirements for each IT system will be established to support this policy.
- CMS will use the Agency's input along with its disaster recovery classifications to establish the priority for restoration of IT systems in the event of failure.
- CMS will store ESI on backup media in order to restore IT systems in the event of a failure.

4.3 IT (Information Technology) Recovery Policy

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.

4.3.1 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.

4.3.2 Scope

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

4.3.3 Responsibility

4.3.3.1 CMS

- CMS/BCCS is responsible for establishing procedures, methods and process documentation that designate actions, roles, and responsibilities to specific personnel to achieve policy compliance.
- 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.

4.3.3.2 Agency

- 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 ongoing communications with CMS/BCCS.

- Each Agency should also establish procedures and assign responsibility to specific agency personnel, such as an IT Recovery Coordinator to achieve policy compliance.
- Each Agency is responsible for:
    - Understanding this policy and the CMS/BCCS IT Recovery Methodology;
    - Determining the appropriate criticality and RTO classification of their applications;
    - Communicating the criticality and RTO classification to CMS/BCCS;
    - Actively participating in local and regional exercises as business needs dictate;
    - The cost of developing, maintaining, and exercising the recovery capabilities of their designated applications.

4.3.4 Policy

- CMS/BCCS will define and maintain the criticality classification and RTO ranges.
- Based on agency input, CMS/BCCS collects and manages criticality classification and RTO information to provide appropriate recovery capabilities.
- CMS/BCCS will provide the IT infrastructure for recovery of Agency designated and justified information systems.
- 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.
- CMS/BCCS will coordinate the recovery exercises for the appropriate IT infrastructure for agency designated and justified information systems and plans.
- Agencies will provide written justification for criticality classification and RTO information to CMS/BCCS for designated information systems.
- Agencies with designated information systems for recovery should schedule yearly local and regional exercises of their recovery plans.
- Agencies will ensure their designated information systems have the appropriate recovery plans and recovery procedures.
- Agencies will coordinate with CMS/BCCS to ensure their criticality classification and RTO information is current.
- Agencies will coordinate and review with CMS/BCCS the feasibility of the recovery plans for their designated information systems.

4.3.5 Methodology

Please find documentation addressing recovery of information processing capabilities in Attachment A - The IT Recovery Methodology.

4.4 **Enterprise Desktop/Laptop Policy**

Department of Central Management Services, Bureau of Communication and Computer Services (CMS /BCCS) establishes the parameters for administering and securing State of Illinois Enterprise Desktop and Laptop Services and Assets.

4.4.1 Purpose

This policy ensures the proper administration of State of Illinois Enterprise Desktop and Laptop Services and Assets.

4.4.2 Scope

This policy applies to State of Illinois Enterprise Laptop and Desktop Services and Assets that are supported by CMS/BCCS. The terms and definitions listed below are meaningful for this policy.

- CMS/BCCS Service Catalog – a collection of CMS/BCCS products and services offered to select State Agencies, Boards and Commissions under the Illinois Governor's jurisdiction.
- State of Illinois Enterprise Desktop and Laptop Services and Assets – services that comprise all PC and Laptop related services including but not limited to the following asserts: desktops, laptops, printers, and other peripheral devices for select agencies, boards and commissions under the Governor's jurisdiction.

4.4.3 Responsibility

- In order to implement this policy, CMS may establish procedures and designate responsibility to specific personnel. Each Agency may also establish procedures and assign responsibility to specific agency personnel to achieve policy compliance.
- CMS/BCCS is responsible for providing maintenance, support and security to the infrastructure and resource established for the Illinois Desktop and Laptop Services and Assets.
- Users are responsible for understanding and adhering to this policy.

4.4.4 Policy

- Each end-user agency will: a) maintain possession of the assets, b) safeguard the assets, and c) maintain inventory reconciliation.
- Changes to the location or user of a fixed asset must be implemented via the CMS/BCCS Enterprise Service Request (ESR) process.
- End-user agencies must promptly report the loss or theft of assets to the proper authorities and to CMS/BCCS Helpdesk

- All desktop and laptop computers shall be configured according to CMS/BCCS approved architecture standards.
- All Enterprise Desktop and Laptop Services are provided in accordance with the CMS/BCCS Service Catalog.
- All requests for exceptions to this policy shall be submitted via the ESR process.

5 Technical Controls

The Technical Controls area of the Security Plan focuses on controls the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for application and data.

5.1 Laptop Data Encryption Policy

This section defines data encryption for State-wide laptop computers.

5.1.1 Purpose

The purpose of the Data Encryption policy is to ensure all sensitive and confidential information that is stored on a state owned mobile digital device is encrypted using CMS strong encryption software.

5.1.2 Scope

This policy applies to all sensitive and confidential data generated, accessed, transmitted or stored on state owned mobile computing devices. Other information may be encrypted at the discretion of the data owner who is responsible for the information. This policy applies only to laptop computers. Subsequent policy releases will address other mobile digital devices.

5.1.3 Responsibility

It is the responsibility of staff to familiarize themselves with this policy and to follow this policy and any corresponding procedures. Agency IT Staff - It is the responsibility of Agency IT staff to familiarize themselves with this policy and to follow this policy and any corresponding procedures.

5.1.4 Policy

- All new laptops issued must be equipped with full-disk encryption.
- Encryption of existing laptops is at the discretion of each Agency.
- Only encryption products approved by BCCS and configured according to standards set by BCCS may be used. It is a violation of this policy for users to encrypt state information with any other products/tools.
- 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 encrypted laptop hard drive(s).

6 Exceptions

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

7 Terms and Acronyms

Terms/Acronyms	Definition
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.
Administrative User	Any person that has been granted special systems administrative authority to manage or maintain computer systems.
Agency Business Application	The application and programs used by the business to process specific business functions and data associated with the application.
Archive	The saving of old or unused files onto off-line mass storage media for the purpose of releasing on-line storage room.
Authorized Individual	A person assigned physical access privileges by a Resource Custodian.
Backup	The saving of electronic information onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction. While most backups are on magnetic tape-based media today, the term “Backup” or “Backup Media” may also reference other backup media technology including but not limited to, Optical (CD, DVD, WORM, etc), virtual tape systems, USB drives, and other removable media.
BRM	Business Reference Model – the repository for capturing, cataloging and maintaining agency business application information.
Broadband	High-speed Internet access—typically contrasted with dial-up access over a modem.
Citrix	A remote access/application publishing product that allows people to

	remotely connect to applications available from central servers.
CMS/BCCS Facility	Any facility that either houses or supports CMS/BCCS Statewide computing operations.
CMS/BCCS Hosted Environments	A CMS/BCCS managed infrastructure used by agencies to store data and run applications.
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.
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).
Content Filtering	The use of a program to screen and exclude from access or availability Web pages or e-mail that is deemed objectionable.
Credential	A card, document, or code that identifies and authorizes the owner physical access to a facility, area or room.
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.
Encryption	The process of transforming information to make it unreadable to anyone except those possessing a key.
ESI	Electronically Stored Information – General term for any electronic information stored in any medium (i.e. hard drives, back-up tapes, CDs, DVDs, jump drives, and any other form of electronic media capable of storing data) that can be retrieved and examined.
Data Owner	The individual(s) responsible for or knowledgeable about how information is generated, created, acquired, transmitted, stored, deleted, or otherwise processed.
Data User	The individual(s), organization or entity that interacts with data for the purpose of performing an authorized task.

Designated Information System	Any system identified as requiring recovery capabilities as defined in the BRM.
Disaster Recovery	The policies, process, and procedures related to preparing for recovery or continuation of technology infrastructure critical to the State of Illinois after a natural or human induced disaster. Disaster recovery focuses on the restoration of IT or technology systems that support business functions that fail in the event of a disaster.
DSL	(Digital Subscriber Line) - a technology for bringing high-bandwidth information to homes and small businesses over ordinary copper telephone lines.
Escorted Access	A limited privilege assigned to an un-authorized individual(s), requiring escort by an authorized individual(s) to physically access CMS/BCCS facilities.
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.
Hotspot	A place within a wireless zone that contains a high concentration of wireless access points and/or routers.
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).
IS	Information System - includes the agency business application and the CMS/BCCS hosted environment.
ITRC	IT Recovery Coordinator – 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.
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.
IT Systems	The hardware and software used to store, retrieve, and manipulate information.
Laptop	A portable, usually battery-operated Personal Computer, small enough to rest on a user's lap.
MIS	Management Information System
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).
Remote access	Connectivity hardware and software including but not limited to: VPN, modem, Citrix, telnet, FTP, and EDI.
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.
Restore	The process of bringing ESI back from off-line media and putting it on an online storage system when the data on the online storage system is lost or corrupted.
RTO	Recovery Time Objective – 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.
Structured Data	Data associated with a business application or system. Data that resides in fixed fields within a record or file. Relational databases and spreadsheets are examples of structured data.
System Owner	The individual(s) responsible for the maintenance and support of the system where the data is generated, accessed, transmitted or stored.
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.
Unescorted Access	A privilege assigned to an authorized individual(s) providing physical access to BCCS facilities via a card (credential), a PIN, and/or a key.
Unstructured Data	Data not associated with a business application or system. Data that does not reside in fixed locations. Examples are word processing documents, PDF files, e-mail messages, blogs and web pages.
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.
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.
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.
Wireless data communication devices	Include personal computers, laptops, routers, and network interface cards connected to any CMS Wireless Zone.
Wireless Service	The provision of wireless computing capabilities within a wireless zone.