DEPARTMENT OF INNOVATION & TECHNOLOGY

IT Coordinator Guide to DoIT Services

Connect to DoIT Website:
https://doit.illinois.gov

Revised: July 2018

Table of Contents

1 OVERVIEW

At the most basic level, the Department of Innovation & Technology is a vendor and agencies are our customers. DoIT provides Information Technology (IT) products and services to designated State of Illinois agencies, boards, commissions, educational institutions, and municipalities (collectively known as “agencies”). The agency may have a person or a group of people who are responsible for the ordering of new IT products and services, maintenance of such, and keeping track of new developments and other ancillary services. These individuals are called **IT Coordinators**.

As an IT Coordinator, you are the key to the whole process. This guide provides the basic knowledge needed to work seamlessly with DoIT in fulfilling agency needs.

.

2 The Department of Innovation & Technology (DoIT)

The Department of Innovation & Technology (DoIT) delivers statewide information technology and telecommunication services and innovation to state government agencies, boards and commissions as well as policy and standards development, lifecycle investment planning, enterprise solutions, privacy and security management, and leads the nation in Smart State initiatives.

DoIT's mission is to empower the State of Illinois through high-value, customer-centric technology by delivering best-in-class innovation to client agencies fostering collaboration and empowering employees to provide better services to residents, businesses, and visitors.

DoIT manages the Illinois Century Network, a service that creates and maintains high speed telecommunications networks providing reliable communication links to and among Illinois schools, institutions of higher education, libraries, museums, research institutions, state agencies, units of local government, and other local entities providing services to Illinois citizens.

DoIT provides improved more rapidly available innovative solutions at an industry efficient price/investment point. This includes but is not limited to

- Improved management of the nearly $1B portfolio of IT investments
- Greater agency oversight of IT services and more transparent rates
- Greater ability to leverage the state's economy of scale in purchasing IT
- A unified IT workforce nearly 1,700 members strong
- Rapid deployment of new agency solutions based on 75-day sprints
- Increased use of new shared enterprise applications for common capabilities
- Increased percentage of citizen and business interaction that are mobile enabled

3 Customer Service Center (CSC)

The Customer Service Center (CSC) operates a combined IT Service Desk (ITSD) and Telecommunications Service Desk dedicated to helping customers deal with operation and maintenance of existing equipment and making informed choices in the purchase of new equipment and services.

The following services are provided by the IT Service Desk

- Create, update, and monitor incident reports of IT repair issues
- Process Service Requests (REQs) for IT end-user support for consolidated and DOIT-supported agencies
- Process service requests for moves, adds, and changes to IT services
- Process customer requested escalation of service requests

The following services are provided by the Telecommunications Service Desk

- Identify cost effective services and equipment – and alternatives
- Consult and recommend the best telecommunications systems for the lowest cost
- Negotiate and expand telecommunications master contracts for equipment and service and, manage vendor performance and service levels under strict terms and conditions
- Provide new telecommunications and data service, systems, and equipment – and monitor warranty periods
- Update DoIT managed inventory and agency billing records
- Create, update, and monitor incident reports of telephone, wireless, and data repair issues
- Use defined metrics to validate and verify the performance, timeliness and value of the products and services delivered by the CSC and contracted vendors

4 IT Service Desk – Customer Support Service Hours

217-524-3648 or 312-814-3648

4.1 Standard Support Service:

- Monday – Friday 8:00 am – 5:00 pm

4.2 After Hours Support Services:

- Limited support is available during non-standard support hours, weekends and holidays
- Available for reporting an IT emergency after standard support hours (i.e., server down, mission critical application not available, large number of customers affected)

4.3 DoIT Production Support: 24x7

- Available for reporting a problem with a scheduled job performance issue
  Call 217-557-1330 or 217-782-1330

4.4 DoIT Data Center After Hours Emergency Escalation and Support:

- Available to agency Technical IT Staff for reporting/escalating emergencies (server down, mission critical application not available, large number of customers affected)
  Call 217-785-8880

5 DoIT Shared Services Teams – Roles and Responsibilities

As DOIT is responsible for the information technology functions of agencies under the jurisdiction of the Governor, it's the IT Coordinator who will interact with the following DoIT Shared Services teams.

5.1 CSC IT Service Desk (Service Requests and Help Desk)

Under direction of the DOIT Chief Customer Officer, IT Service Desk agents (ITSD agents) provide computer related services to thousands of end users at the consolidated state agencies and state boards and commissions under the Governor. ITSD agents perform a variety of tasks that include the processing of Service Request Forms (REQs). ITSD agents assign tasks to appropriate DOIT Shared Services teams, and upon customer request DOIT shall provide reasonable escalation when necessitated.

The ITSD agents are available to re-set passwords, trouble-shoot basic repair problems, provide Tier 1 help desk assistance with fundamental technology services, and monitor issues until resolution. Each incident is identified, recorded, categorized, assigned the appropriate priority, tasked to appropriate DOIT Shared Services teams, and tracked until resolution. When necessary an incident will be escalated based on criticality and the overall impact of the incident.

In major outage situations, ITSD is responsible for notification to DOIT leadership, agency CIOs, and other key agency personnel. These incidents are opened as a "MORT" (Major Outage Response Team) which is assigned to a dedicated Duty Manager. Updates are provided throughout the "MORT" by the Duty Manager and/or ITSD agent(s).

5.2 Personal Information Management (PIM – Email Services)

Under direction of the DOIT Chief Technology Officer, the PIM team is responsible for maintaining Enterprise e-mail services (including email services on state-issued mobile devices), Enterprise Fax Service, Enterprise List Server Service, e-mail archiving and Spam filtering.

5.3 Data Center Operations

Under direction of the DOIT Chief Technology Officer, the Data Center Operations team is divided into four areas.

- **Enterprise Storage and Backup** – staff is responsible for maintaining storage and backups for services provided
- **UNIX** – staff is responsible for maintaining UNIX server based services
- **Wintel** – staff is responsible for maintaining hardware and virtual server based services
- **Mainframe** – staff is responsible for maintaining mainframe server based services

5.4 LAN Services

Under direction of the DOIT Chief Technology Officer, the LAN Services team is responsible for maintaining network connections via LAN connectivity.

5.5 End User Computing (EUC)

Under direction of the DOIT Chief Customer Officer, the End User Computing team supports the configuration, installation, maintenance, troubleshooting, break/fix and upgrades of personal computers and the associated software and peripherals.

- **EUC Incident Management** team executes with the goal to remotely resolve customer EUC issues without dispatching field technicians
- **EUC Service Management** team is responsible for reviewing, processing, and managing EUC service requests. The team specializes in providing ownership and oversight of service requests to ensure a "complete service" is provided to the customer.
- **EUC Field Operations** team is responsible for providing on-site customer support.
- **EUC Staging** team is responsible for fulfilling incidents and service requests requiring hardware asset inventory
- **EUC Imaging** team is responsible for fulfilling incidents and service requests requiring software asset inventory

5.6 Asset Management

Under direction of the DOIT Chief Customer Officer, is responsible for maintaining State of Illinois hardware inventory purchased by DOIT.

- Inventory information will be used to track equipment pertaining to adds, moves and transfers to surplus and to conduct yearly inventories for verification.

5.7 Business Services

Under direction of the DOIT Chief Financial Officer, the Business Services staff is responsible for paying vendors (for the equipment/services provided) and, in turn, billing the agencies for the products and services they use. Each agency has a billing account provided by DOIT and receives monthly statements identifying charges for equipment purchase, rental, maintenance, service, and usage.

6 Appointing IT Coordinator

Each agency has unique needs that must be considered when recommending and providing service. DOIT requires that each agency appoint an IT Coordinator, and based on agency operations, multiple coordinators may be appointed and assigned individual and/or overlapping responsibilities.

DOIT considers an IT Coordinator to be the agency's authorized submitter for all requests for information technology products and services. This individual must have sufficient agency knowledge and authority to fulfill the responsibilities defined under "IT Coordinator Roles and Responsibilities". It is essential that an IT Coordinator develop a working knowledge of the Remedy application used to process orders, manage help desk incidents, and complete IT inventory billing.

An agency head (Agency Director, Chairman of a Commission, Chancellor of a University, etc.) must appoint all IT Coordinators using the required "DOIT Customer Registration" form that identifies the coordinator, provides his/her contact information, and delegates his/her assigned level of authority to submit service orders (thus obligating/expending the agency's IT funds). Appointment requires the agency head's signature.

All signed "DOIT Customer Registration Forms" appointing new IT Coordinators or changing the authority of an existing coordinator should be sent to DOIT as addressed below.

DOIT Agency Relations
120 West Jefferson Street, 1st Floor
Springfield, Illinois 62702-5103

DOIT Agency Relations maintains a database of all agency coordinators and their delegated spending authority. An agency may appoint multiple IT Coordinators: their individual duties and spending authority may be identical, or each IT Coordinator may be responsible for different service areas.

DOIT may host various conferences and training sessions throughout the year that will benefit new coordinators by instructing them on the basics of pricing; forms completion; ordering; and Remedy inventory, tracking, billing, and reporting.

6.1 IT Coordinator Roles and Responsibilities

- Review annual listing of VIP employees provided by the IT Service Desk.
- Review and interpret DOIT service notifications. IT bulletins provide notification of important due dates, changes in service offerings, pricing updates, and other critical information.

- Convey the agency's IT needs (with collaboration of DoIT resources as needed) to DoIT via a service request.
- Determine user service and equipment needs based on established agency guidelines.
- Review and approve IT service requests within the agency to ensure compliance with DOIT, procurement, and agency guidelines.
- Work with the agency-appointed State Procurement Officer to budget for IT expenditures, ensure that adequate funds are available, and verify that the proper accounting unit code numbers (known as Accounting Unit Code and/or Billing Code) are used when requesting IT products and services.
- Coordinate with DOIT Shared Services teams on IT/Telecom projects and services. IT Coordinators must:
  - Submit service requests that allow sufficient time for delivery/installation.
  - Provide early notification of all major projects, moves, and other non-routine service requests.
  - Submit due dates, studies, plans, and other related documentation for any project.
- Review and familiarize oneself with the DOIT Website and the Remedy OnDemand (ROD) MyIT Training in order to track service requests and help desk incidents, and to verify inventory assets.
- Assist DOIT in maintaining up-to-date inventory records of agency IT/Telecom equipment and services.
- Notify DOIT of any changes in agency Coordinator status and submit annual verification of agency coordinators, their contact information, and levels of spending authority. (The annual Coordinator verification process is initiated by DOIT and agency response is mandatory for audit purposes.)
- Review annual listing of VIP employees provided by the DoIT Service Desk.
- Review and interpret DOIT service notifications. IT bulletins provide notification of important due dates, changes in service offerings, pricing updates, and other critical information.

7 Requesting IT Services

Agencies obtain e-mail, security, software, personal computing services, and any other services by submitting through the Remedy OnDemand (ROD) system. The Remedy OnDemand system presents services through the Digital Workplace Catalog.

When submitting requests, Coordinators should submit requests that allow sufficient time for delivery of the requested service. Coordinators may also familiarize themselves with the various services by visiting the DOIT Website and selecting Service Catalog under Services. The ITSD agents can assist with request completion and the most frequently submitted requests are listed below.

7.1 Selecting the Correct Catalog Request

Providing accurate and complete information on the correct form allows the DOIT Shared Services teams the ability to complete service requests accurately. For specific details concerning service offerings, visit DOIT Services Catalog for more information.

All questions pertaining to service requests can be emailed to the CSC IT Service Desk at the following e-mail address.

DOIT.ESR.AllAgencies@illinois.gov

7.1.1 Employee Onboarding

This catalog service is used for an employee who is ***new to the agency, or an employee who is transferring into the agency***. Use this selection when you have **a *new or transferring employee*** and you need to add, change, delete, or enable any of the following services:

- Email Services
- Permission Services - access to files, network account and applications
- Business Applications supported and provided by DoIT. Many agencies have specific applications supported by their own application personnel. Prior to submitting, check with your agency application personnel to verify who supports the application.
- Hardware, such as PC, Monitors, Laptop, Tablet, etc., and whether it is to be installed, reimaged, moved, or just reassigned.
- Software, if any needs to be installed on the equipment designated. If the software needed does not appear in the list of choices, indicate what software and version is needed in the Detailed Description of Services Requested.
- Mainframe Account – whether an account is to be created, modified or deleted. You will choose the type of user (whether TSO or IMS), and what Mainframe Applications should be added or removed for this user.

7.1.2 Employee Offboarding

This catalog service is used for an employee who **is *leaving your agency.*** Use this selection when you have ***an employee who is leaving*** and you need to delete and/or re-assign the following services:

- Email Services - Remove service (if needed indicate re-assignment of user's email records to supervisor)
- Permission Services – Remove access to files, network account and applications (if needed, indicate re-assignment of user's personal drive records to supervisor)
- Business Applications - Supported and provided by DoIT. Many agencies have specific applications supported by their own application personnel. Prior to submitting, check with your agency application personnel to verify who supports the application.
- Hardware – If any equipment, such as PC, Monitors, Laptop, Tablet, etc., is to be reimaged, moved, or just reassigned to supervisor.
- Software - If any software needs to be moved, or just reassigned, indicate what software and version is needed in the Detailed Description of Services Requested.
- Mainframe Account – Remove service. If account is to be deleted, you will choose the type of user (whether TSO or IMS), and what Mainframe Applications should be added or removed for this user.

7.1.3 Existing Employee – Multiple Services Requested

This catalog service is used for a currently employed individual who needs any combination of the multiple services listed. If an existing employee only needs one of the services, you may also utilize one of the other catalog requests. Use this selection when you ***have an existing employee*** and you need to add, change, delete, or enable any of the following services:

- Email Services
- Permission Services - access to files, network account and applications
- Business Applications - Supported and provided by DoIT. Many agencies have specific applications supported by their own application personnel. Prior to submitting, check with your agency application personnel to verify who supports the application.
- Hardware - If any equipment, such as PC, Monitors, Laptop, Tablet, etc., is to be reimaged, moved, or just reassigned.
- Software - If any needs to be installed on the equipment designated. If the software needed does not appear in the list of choices, indicate what software and version is needed in the Detailed Description of Services Requested.
- Mainframe Account – Whether an account is to be created, modified or deleted. You will choose the type of user (whether TSO or IMS), and what Mainframe Applications should be added or removed for this user.

7.1.4 Employee Name Change Request

This catalog service is used for a currently employed individual who requires a name change. Use this selection when you ***have an existing employee*** requiring a name change and you need to change any or all of the following services:

- Email Services
- Permission Services - access to files, network account and applications
- Business Applications - Supported and provided by DoIT. Many agencies have specific applications supported by their own application personnel. Prior to submitting, check with your agency application personnel to verify who supports the application.
- Hardware - If any equipment, such as PC, Monitors, Laptop, Tablet, etc., is to be reassigned.
- Software – If any software needs to be re-assigned, indicate what software and version is needed in the Detailed Description of Services Requested.
- Mainframe Account – If a mainframe account is to be modified, specify the mainframe ID and type of user (whether TSO or IMS).

7.1.5 Email Request (Enterprise Email)

This catalog service is used for an employee who **requires various email services**. Use this selection when an employee for whom you need to add, change, delete, or enable any of the following services:

- Mailboxes hosted on DoIT managed Microsoft Exchange high availability servers
- Enterprise mail routing, spam filtering, and virus protection
- Microsoft Outlook Client software
- Calendaring and scheduling
- Enterprise email archiving
- WebMail access
- Standard disaster recovery
- File transfer utility (described below)
- Email journaling (all email transmitted in the enterprise email system is kept for one year for investigative purposes)
- *Illinois.gov* email address and a Statewide Unified Directory
- Availability through State owned mobile devices (as part of the centralized email environment)

7.1.6 Permission Request

This catalog service is used for an employee who **requires access to a file path and network account services**. Use this selection when an employee for whom you need to add, change, delete, or enable any of the following services:

- Network Account
- Shared Folder /File or Drive Access
- Security Group
- Internet Access
- Remote Access – Citrix
- Remote Access – VPN
- SQL
- UNIX

7.1.7 Software Request

This catalog service is used for an employee who requires software services. Use this selection when you need to add, change, re-assign or remove any of the following services:

- Desktop Software – For complete list and pricing please visit DoIT Website Desktop Software .
- Agency Software Bundles – For a complete list of your agency's specific bundles, please visit Agency Software Bundles
- If the software needed does not appear in the list of choices, indicate what software and version is needed in the Detailed Description of Services Requested.

7.1.8 Application Request

This catalog service is used for business applications that are supported and provided by DoIT. Many agencies have specific applications supported by their own application personnel. Prior to submitting, check with your agency application personnel to verify who supports the application.

- Adobe Reader Extensions Service
- CPS – Central Payroll System
- Cryptography Services
- EPASS – Electronic Pay Stub System
- Enterprise Email service option for Priority Disaster Recovery
- Enterprise Fax Service
- Enterprise List Server Service
- eTime – Central Time & Attendance System
- SAP – Enterprise Resource Planning
- SIREN

7.1.9 Hardware Request (Single)

This catalog service is used for a single employee who requires changes to PC equipment (Desktop / Laptop / Monitor, etc.). Use this selection when a single employee needs the add, change, or removal of the following services:

- New equipment (requires GOMB approval)
- Used equipment
- Reimage of equipment
- Move equipment
- Reassignment of equipment (No technician support provided. Documentation update only)

NOTE: Remember to attach the approval from the Governor's Office of Management and Budget (GOMB) for the new equipment prior to submission.

7.1.10 Hardware Request (Multiple)

This catalog service is used for multiple equipment for *up to ten (10) users* at one location that require changes to PC equipment (Desktop / Laptop / Monitor, etc.). This request may be used to request either new or used equipment, and to request installation of software on that equipment prior to installation. Use this request to indicate the PC equipment (Desktop / Laptop / Monitor, etc.) and any appropriate peripheral equipment.

NOTE: Remember to attach the approval from the Governor's Office of Management and Budget (GOMB) for the new equipment prior to submission.

7.1.11 Move Hardware Request (Multiple)

This catalog service is used for multiple equipment for *up to ten (10) users* at one location. that require relocating PC equipment (Desktop / Laptop / Monitor, etc.) and any appropriate peripheral equipment.

7.1.12 Reassign Hardware Request (Multiple)

This catalog service is used for multiple equipment for *up to ten (10) users* at one location. that require re-assigning PC equipment (Desktop / Laptop / Monitor, etc.) and any appropriate peripheral equipment.

NOTE: No technician support provided. The purpose of re-assigning equipment is for documentation purposes only.

7.1.13 Reimage Hardware Request (Multiple)

This catalog service is used for multiple equipment for *up to ten (10) users* at one location, that requires re-reimaging of PC equipment (Desktop / Laptop).

7.1.14 Mainframe Access Request

This catalog service is used when an employee requires access changes to mainframe computing services. The mainframe includes hardware and software to ensure data is accurate and available on demand to authorized users. Use this selection when requesting mainframe access for TSO or IMS to access mainframe applications. The following lists various Language & Tools

- **BlueZone:** Connects to TN3270 server using a TELNET connection and emulates IBM3270 mainframe terminal. It provides full TN3270E protocols, SSL/TLS connection, printer session functionality, and scripting capabilities
- **CA-Scheduler:** Provides workload automation of traditional job scheduling encompassing online disciplines, integration with business applications and scheduling based on external events
- **CICS:** Customer Information Control System is a transaction processing system designed for both online and batch processing activity
- **DB2:** DoIT operates shared database environments using DB2 in the enterprise data center. State departments access DB2 data using Structured Query Language (SQL) via standard interfaces such as CICS, QMF or call attach. Remote access is also available via middleware products such as DB@ Connect and QMF for Windows

- **DB2 Administration Tool:** Automates routine DBA administration tasks including object change management, security, reporting, data movement and placement
- **Debug Tool:** Used to examine, monitor and control the execution of C, C+ and Cobol programs
- **DFSORT:** High-performance sort, merge copy, analysis and reporting product
- **Fault Analyzer:** Helps to identify, analyze and fix the problems associated with failing applications
- **File Manager:** Toolset for working with mainframe datasets and DBS and CICS data
- **Finalist:** Finalist is an address cleansing tool used mainly in batch processing. The address file is run through Code 1 and cleansed for mailings. This tool can also be used through interactive processing in CICS
- **FTP:** FTP uses TCP/IP as a standard way of transferring files across the Internet and between computers
- **FTPS:** SSH is a security protocol for logging onto a remote that provides an encrypted session for transferring files and executing server programs
- **ISPF:** A panel application navigated by keyboard that includes a text editor and browser and functions for locating and listing files and performing other utility functions
- **JCL:** Job Control Language to manage the production control for mainframe programs
- **Language Environment:** This provides a common environment for all language environment-conforming high-level language (HLL) products
- **Mobius:** Comprehensive report-management viewing, archival and print distribution system covering every aspect of report life cycle
- **MQ Series**: Middleware used for messaging and queuing that enables programs to communicate with each other across a network of unlike components such as processors, subsystems, operating systems and communication protocols
- **Netview Access Services:** Allows customers to simultaneously log on to multiple applications (CICS, TSO, etc.) without logging on and off
- **Omegamon for DB2:** Insight is an interactive performance monitor that enables the user to specify a DB2 subsystem to monitor including system summary, active threads, system activity review, user activity review and user activity trace
- **QMF:** QMF Enterprise Edition allows easy-to-use visual query building that enables users of all skill levels to easily create their own reports accessing DB2
- **TSO:** Allows customers to create an interactive session with the mainframe
- **UNIX Systems:** UNIX on the mainframe utilizing the Java programming language
- **VPS:** This feature is the basis for a total print serving solution for the z/OS environment. Delivers improved efficiency with the flexibility for high volume, high-speed printing from anywhere in the network

7.1.15 SharePoint Request

This catalog service is used when an agency is interested in internal collaboration, external collaboration, organizational portals, business process workflow, web content management and business intelligence. This hosted service is ideal for storing project documents in a central location and sharing them with others. By using SharePoint lists, libraries and web parts, team members can work more efficiently and productively. DoIT offers both an Internal and an External farm depending on the type of collaboration. Use this request for SharePoint services.

7.1.16 Storage Hardware Request

This catalog service is used for midrange storage services. Midrange storage services provides both quick and ready access as well as long-term storage that will not be accessed on a daily or frequent basis. Use this selection when requesting midrange storage changes.

- Backup and recovery of storage data
- Authorization to users and advanced access management to provide access to storage
- Monitoring and security scanning for stored files for any potential electronic threat
- Virus protection services for servers managing and accessing the data stored on these storage devices

7.1.17 Server Hardware Request

This catalog service is used for midrange hardware services. The management of servers, storage and backup/restore services for executive branch departments within the State of Illinois. It includes installation, deployment, maintenance and support of the operating system (OS), web server and application server software. Use this selection when midrange hardware service requires an add, change, or removal.

7.1.18 Server Software Request

This catalog service is used for midrange software services. The management of servers, storage and backup/restore services for executive branch departments within the State of Illinois. It includes installation, deployment, maintenance and support of the operating system (OS), web server and application server software. Use this selection when midrange software service requires an add, change, or removal.

7.1.19 Mainframe Hardware Request

This catalog service is used for mainframe hardware services. Mainframe computing services are supported by mainframe computers, data storage devices and many special-purpose devices. The mainframe includes hardware and software to ensure data is accurate and available on demand to authorized users. Each data center has redundant power, climate control, card-key access doors, video monitoring and full-time staffing. Use this selection when mainframe hardware service requires an add, change, or removal.

7.1.20 Mainframe Software Request

This catalog service is used for mainframe software services. Mainframe computing services are supported by mainframe computers, data storage devices and many special-purpose devices. The mainframe includes hardware and software to ensure data is accurate and available on demand to authorized users. Each data center has redundant power, climate control, card-key access doors, video monitoring and full-time staffing. Use this selection when mainframe software service requires an add, change, or removal.

7.1.21 Security Software Request

This catalog service is used for security related software services. Use this selection when software related to security type of services requires an add, change, re-assignment or removal.

7.1.22 Software Packaging Request

This catalog service is used for software packaging services when individual software files or resources need to be packaged together as a software collection that provides certain functionality as part of a larger system. Use this selection when software packaging service requires an add, change, or removal.

7.1.23 Network Data LAN Request

This catalog service is used for Local Area Network (LAN) services. Typically, wired or wireless services provide LAN infrastructures within a building or agency environment enabling data communication among local computing and printing resources within an organization. These services support the infrastructure components and resources beginning where the end device connects into a wall plate. Use this selection when LAN service requires an add, change, or removal.

7.1.24 Network Data WAN Request

This catalog service is used for Wide Area Network (LAN) services. Typically, configuration of wired or wireless services provide WAN infrastructures between buildings or agency's environments enabling data communication among local computing and printing resources within an organization. These services support the infrastructure components and resources by connecting LANs to various hubs allowing access to internet, centralized state computer networks and non-state computer providers. Use this selection when WAN service requires an add, change, or removal.

7.1.25 Local Printer Request

This catalog service is used for a local printer services. Typically, a local printer is directly connected to an individual's PC or laptop. Use this selection when a single individual requires an add, change, or removal of a local printer.

7.1.26 Network Printer Request (Single or Multiple)

These catalog services are used when part of a workgroup or network of computers can all access the same printer at the same time. A network can request installation services and use of networked multi-function office devices in support of, among other responsibilities, printing services in conjunction with the many services it provides to the public. The single catalog can be used for one network printer changes, whereas the multiple catalog service is used for multiple equipment for *up to ten (10) users* at one location.

8.0 MyIT – Digital Workplace (Catalog)

The following information will assist with completing the Request Details, Agency Information and Task Coordinator. When completing a specific catalog selection, complete the individual sections unique to each of the catalog services.

Request for - Enter the name of the person within agency who shall receive the service. If you are unable to locate the person then leave it as yourself.

Request Details – If you were unable to locate the individual, then select “No” and populate the Guest Information of the individual.

Guest Information – It is important to provide complete Guest Information to ensure proper updating of the global address book, Active Directory (AD) and other accesses to systems ensuring the correct attributes are associated to the person. If a Middle Initial is available then please provide. Street Address should be the proper street address associated to “911” and not such items as a P.O. Box number and a building name.

Agency – Select your agency name from the drop down.

Account - Agency specific code referenced in DOIT billing statement (Required)

Billing Code (3 digit) – Agency billing/budget code. (Optional)

Agency Tracking Number – If the approval for this request results from an existing internal agency tracking system, enter the applicable system’s assigned reference number. (Optional)

Task Coordinator - Name of the person who will be notified by Shared Services Teams if more details are needed on the Service Request. Typically, this could be the supervisor of the individual receiving the service or the individual knowledgeable about the service request. (If left blank ITSD support staff will assume the IT Coordinator will be the Task Coordinator•)

If you are unable to locate the person through filtering and drop-down list, then type in the task coordinator information.

8.1 Approving Catalog Request

Once the request has been submitted, then an IT Coordinator must approve the request.

9 Routine IT Service Request Process

1. The end user (or supervisor) generates a request to the agency IT Coordinator.

2. The IT Coordinator creates the request through the Remedy OnDemand – MyIT Digital Workplace catalog. (In some instances, LAN Administrators or agency designated personnel will perform this step).

3. An IT Coordinator will approve the request through the Remedy OnDemand – MyIT Digital Workplace catalog. By approving the request, the IT Coordinator gives authorization for these services to be rendered and billed to the agency.

4. The IT Service Desk (ITSD) agent reviews the request in Remedy, evaluates the request, clarifies any discrepancies, and routes it to the appropriate DOIT Shared Service team(s). (Service Requests are worked in the order in which they are received.)

5. The ITSD agent coordinates the request with the appropriate DOIT Shared Services team(s).

6. Equipment delivery, installation work and/or services requested are assigned and monitored by the designated DOIT Shared Services teams.

8. The Asset Management team updates inventory records for DOIT Business Services to generate billing to the agency.

9.1 Service Request - Delivery Expectations

The service request delivery expectations dates are based on “Low” urgency expectations to enable customers to forecast anticipated services. Service requests are worked on a “first in/first out” basis and you should allow sufficient time when submitting/approving request to your delivery date. Please use the below chart as a tool to assist with managing and planning your submitted service requests.

Description of Service	Business Days to Complete						
	1 - 5	5 - 10	10 - 15	15 - 20	20 - 25	25 - 30	30 +
New Employee - Add (Email/Network Account)	■						
New Employee - Add (Email/Network Account/Software/Hardware Standard		■					
New Employee - Add (Email/Network Account/Software/Hardware Non-Standard)						■	
Employee - Delete (Email/Network Account)	■						
Employee - Delete (Email/Network Account/Software/Hardware Changes)			■				
Email Add/Changes	■						
Security Permission Changes (Network Account/File Drive Access)	■						
Hardware Desktop/Laptop /Peripherals - Install (Standard) *New / Reissued Equipment from BCCS Warehouse						■	
Hardware Desktop/Laptop/Peripherals - Install (Non-Standard) *Requires Special Hardware Configurations other than Standard issued - includes 30" Monitors							■
Hardware Desktop/Laptop/Peripherals - Move *Equipment already in possession of agency, needs moved to different location					■		
Hardware Desktop/Laptop - Change *Reimage of current equipment located at agency			■				
Hardware Desktop/Laptop/Peripherals - Remove *Equipment that is to be returned to the BCCS Warehouse and removed from agency inventory						■	
Software Install/Change - Desktop (Standard)			■				
Software Install - Desktop (Non-Standard) *Agency Owned Software to be Procured *CMS/BCCS Owned Software to be Procured							■
Software Server - Change		■					
LAN - Change (Existing Wiring)		■					
LAN - Change (Existing Wiring - Southern Regions)			■				
LAN - Install (Non-Existing Wiring) *Availability of Vendor for Installation							
Network Printer Installation			■				

9.2 Service Request Escalation Process

1. Only the CIO of an agency may call the IT Service Desk (ITSD) and ask to speak to an IT Service Desk Manager or email the DOIT.ESR.AllAgencies@illinois.gov to initiate an escalation. The email should contain supporting documentation for escalation.

2. CIO provides the Remedy Service Request ticket number (if known).

3. CIO provides the justification or business need for the escalation.

4. The ITSD creates a work log entry to include the provided information.

5. The ITSD service processing team contacts the DOIT Shared Services team and/or technician to notify them of the escalation.

6. The assigned DOIT Shared Services team and/or technician is/are required to contact the customer with an update and an estimated time of completion. The DOIT Shared Services team will increase the priority based on the required completion.

7. The CIO/IT Coordinator may follow-up with the IT Service Desk Manager or ITSD processing team (DOIT.ESR.AllAgencies@illinois.gov) if the DOIT Shared Services team and/or technician does not respond or make an onsite visit by the projected ETA for completion.

8. The IT Service Desk Manager escalates to the next level of DOIT Management.

10 Reporting Problems

217-524-3648 or 312-814-3648

One of the duties IT Coordinators may encounter is “Incident Reporting.” IT Coordinators may be the point of contact for users experiencing difficulties related to office automation and other IT related issues.

Note: Not all agencies use their IT Coordinators to report IT related problems. Please follow respective agencies’ current practices.

DoIT Managed Agencies pay a monthly fee for End User Support that covers faulty PC and printer equipment. Every attempt will be made to repair faulty equipment. If equipment is deemed un-repairable or if the cost to repair exceeds current value of the device, then the IT Coordinator will be required to submit an ESR for replacement.

Items that are not supported by the IT Service Desk include fax machines, copy machines, toner cartridges and other office-related machines. If asked by staff to support or report problems with these devices, IT Coordinators will need to follow their agency guidelines.

Note: Problems with telephone lines and equipment, data lines, pagers, cellular and Blackberry devices should be reported to the CSC Telecom Repair Desk.

IT Coordinators should instruct users to provide the following information when contacting the IT Service Desk for assistance.

- Inventory tag number
- Product name, version or model of any hardware or software involved
- Any error codes or symptoms observed
- Statement whether the problem is intermittent or continuous
- Number of people impacted by the problem
- Location and the person to contact for follow-up

10.1 Checking Status of REQ/Incident Ticket

1. Call the IT Service Desk or send email to DoIT.HelpDesk
2. Give the ITSD agent the Remedy Incident ticket number (if known).
3. Request the most recent status update from the Remedy Incident ticket work log.
4. Request to be contacted by the assigned DOIT Shared Services team and/or technician if the work log is not current.
5. Call the IT Service Desk and ask to speak to a manager if the assigned DOIT Shared Service team and/or technician does not respond within a reasonable timeframe.
6. Ask the IT Service Desk Manager to escalate the Remedy Incident ticket (see 'Incident Ticket Escalation Process').

10.2 REQ/Incident Ticket Escalation Process and Complaints

Incident Escalations

Once the help desk receives a request for an escalation, the ticket is flagged in Remedy and the tech and group manager are contacted to let them know of the request.

This is the process that should be followed by a LAN/IT Coordinator or End User to follow up on the status of or request an escalation of an existing help desk ticket.

Send email to DoIT.helpdesk@illinois.gov
Flag email as high priority (!)
Subject: Escalation Request - INC Ticket #

Complaints

Contact ITSD Management via email or phone call – include as much information about the issue as possible – date/time, names, ticket numbers, etc.

Liz McComb
IT Service Desk Manager
liz.mccomb@illinois.gov
217-782-1490 (o)
217-685-9898 (c)

Deb Harvey
Customer Service Officer
deb.harvey@illinois.gov
217-782-8220 (o)
217-494-5870 (c)

10.3 Missing or Stolen IT Equipment

1. Contact the IT Service Desk as soon as aware an asset is lost or stolen.

2. Please provide asset inventory tag number and person assigned asset.

3. If you believe the asset was stolen, a police report is required. If asset is believed to be lost or misplaced, no police report is required. (Service Desk representative will ask you to forward the police report to DoIT.HelpDesk@illinois.gov)

11 CSC Management Contact Information

CSC Manager
Deb Harvey
deb.harvey@illinois.gov
O: 217-782-8220
C: 217-494-5870

IT Service Desk Manager
Elizabeth (Liz) McComb
liz.mccomb@illinois.gov
O: 217-782-1490
C: 217-720-9136

IT Service Desk Supervisor
Monica Houston
monica.houston@illinois.gov
O: 217-524-4623
C: 217-725-4818

IT Quality Assurance & Service Processing
Gary Wasilewski
gary.wasilewski@illinois.gov
O: 217-557-8000

Locations and Other Contact Information

CSC – IT Service Desk
120 West Jefferson – 2nd floor
Springfield, Illinois 62702-5103

CSC – IT Service Desk
JRTC – 3rd floor
100 West Randolph Street
Chicago, Illinois 60601-3219

Email Address: DoIT.helpdesk@illinois.gov
FAX: (217) 524-0755
TTY: (217) 277-5669

12 Information Technology Equipment, Property Control and Software

12.1 Tagging DOIT Owned PC Equipment

By State statute, IT hardware purchased by DOIT that meets the Property Control inventory threshold will be tagged and inventoried by DOIT. A unique six-digit property control bar code tag is issued to this equipment upon receipt and the inventory record is added to the DOIT inventory system. Agencies should not record DOIT (C or L tag) equipment on their property control records or place their official agency inventory tag on that equipment.

12.2 IT PC Equipment Inventory Certification

Agencies are required to complete an inventory of their DOIT PC equipment at the end of each calendar year. The December monthly billing report will serve as the official year-end inventory report for this purpose. An inventory certification form will also be included with the December bill. This year-end certification must be completed, signed and returned within 45 days of receipt.

12.3 Protection against Theft

Each agency is responsible to protect IT equipment from theft. Agencies will be responsible for filing a police report and notifying the IT Service Desk if equipment is stolen. DOIT requires that a service request along with the police report be submitted to remove stolen equipment from inventory. An additional service request will need to be submitted to obtain replacement equipment. Agencies are responsible for the replacement cost of stolen equipment as well as the remaining unpaid balance of any DOIT equipment lease or finance agreement.

12.4 Software

Agencies that procure and manage their own desktop software inventories are responsible to ensure that a valid license is available. Exceptions are DOIT managed software applications that include Microsoft Enterprise Agreement (MSEA), Bluezone, McAfee Anti-Virus, and Entrust/PointSec Disk Encryption (Laptop). Requests involving the installation of software products must identify whether the software requested is agency-owned or DOIT-owned/managed and include the version(s) of the software requested. For agency owned software, technicians will require an agency license key prior to installing software. For DOIT owned/managed software, DOIT will verify the license requested. If ownership cannot be determined, DOIT will procure a new license and bill back the requestor via the SSRF. DOIT will only install licenses requested on the IT Service Modification Addendum.

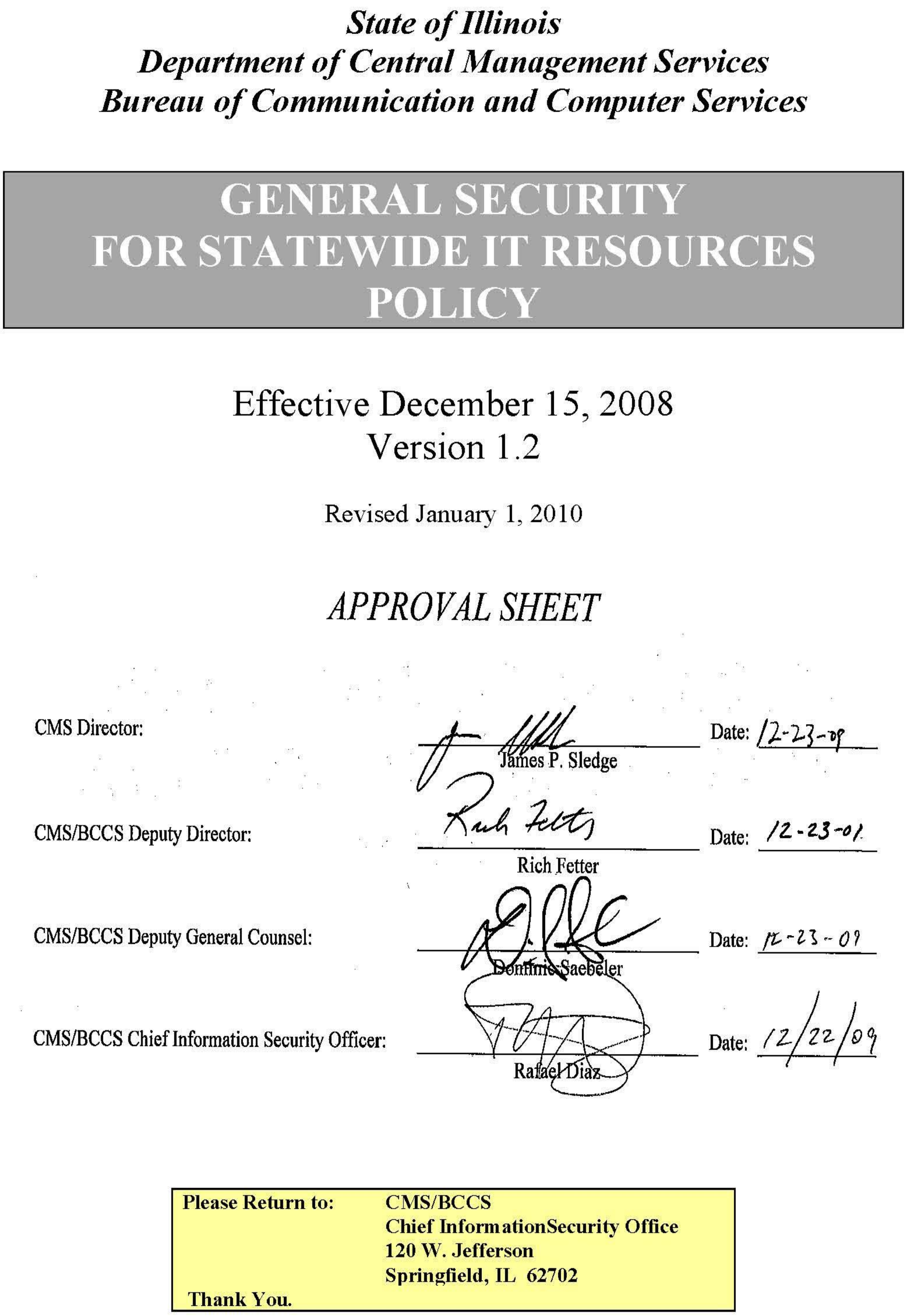
- Laptop Encryption
    - Windows 7 operating system comes with the encryption software already installed
    - Other laptop operating systems *must* have the encryption software installed by technician

13 General Security for Statewide IT Resources Policy

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

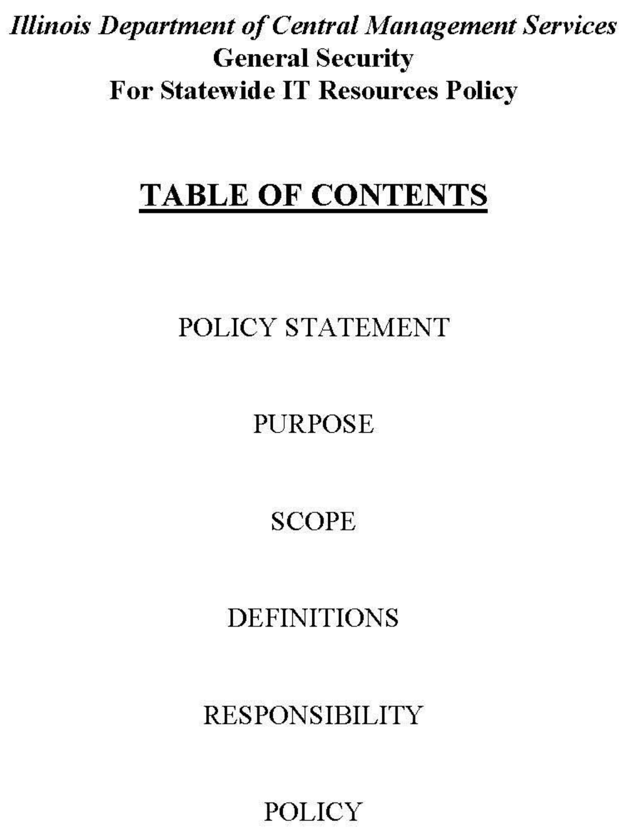
CMS Director: James P. Sledge Date: 12-23-09

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.

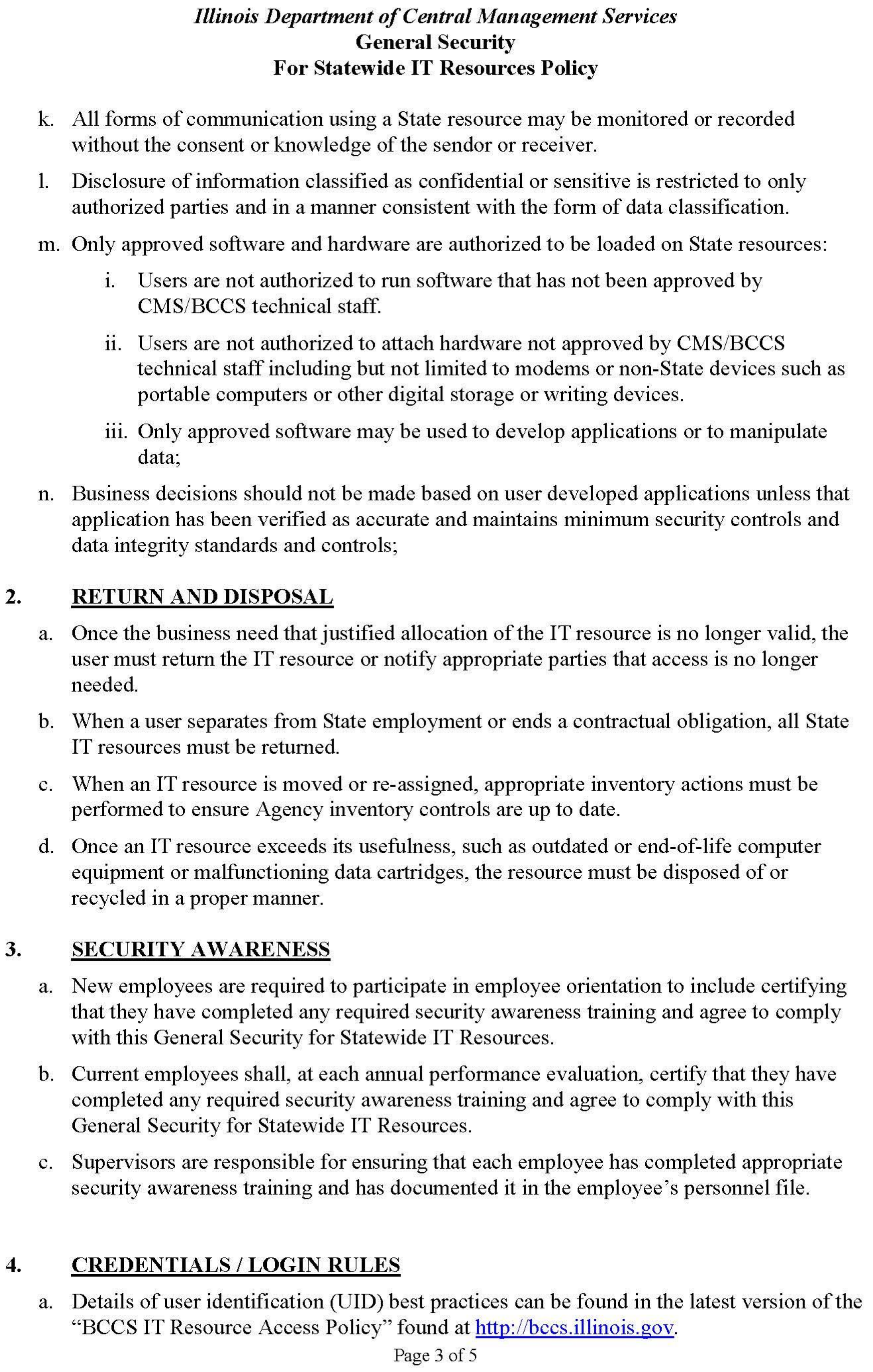
f. Use of IT resources may be filtered, monitored, suspended, or terminated at the discretion of the Resource Custodian or designee, or Law Enforcement based on approved criteria including but not limited to job duty changes, access inactivity, security concerns, policy violation(s), or other events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

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. <u>SECURITY AWARENESS</u>

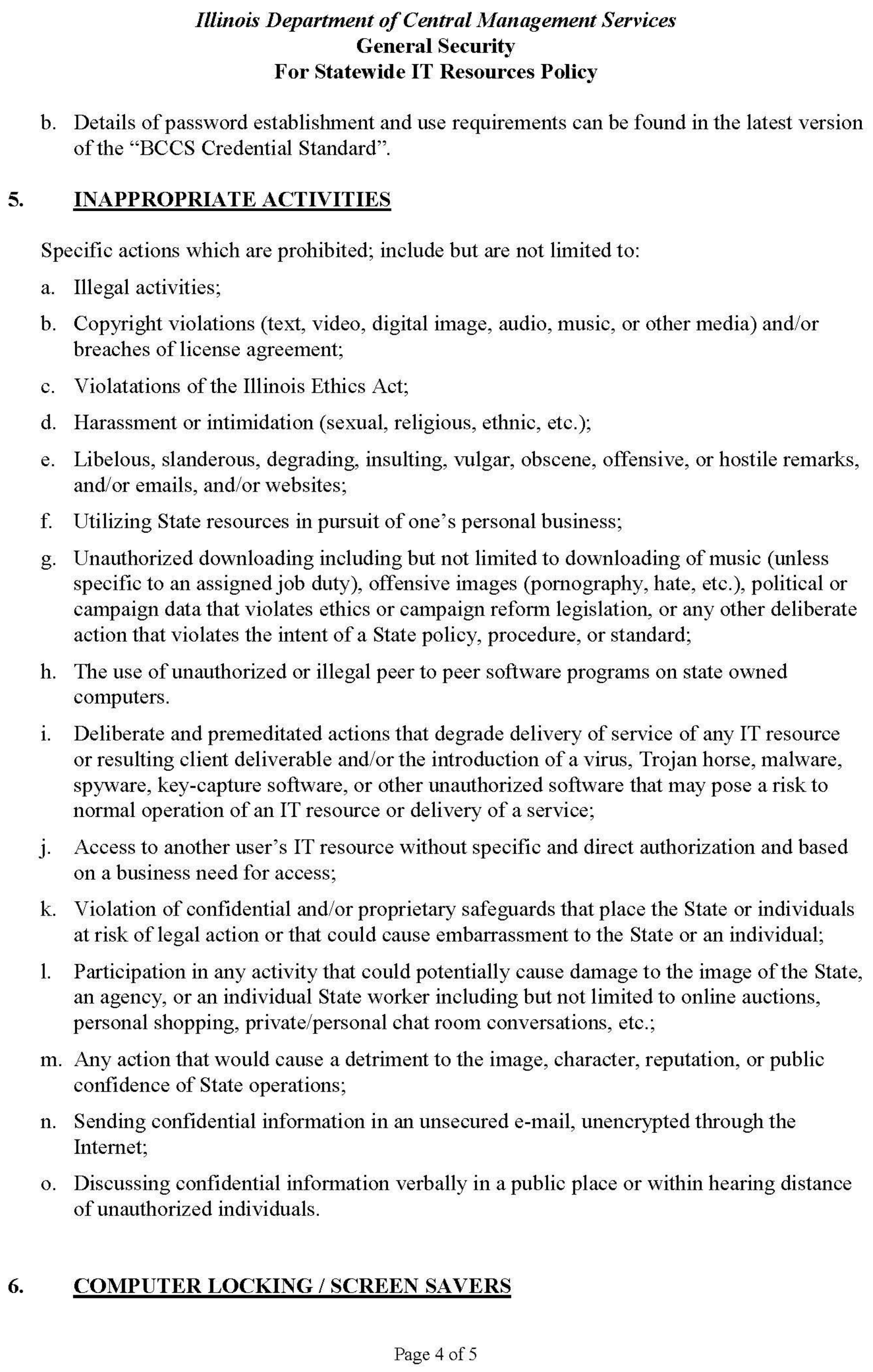
a. New employees are required to participate in employee orientation to include certifying that they have completed any required security awareness training and agree to comply with this General Security for Statewide IT Resources.

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. <u>CREDENTIALS / LOGIN RULES</u>

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;

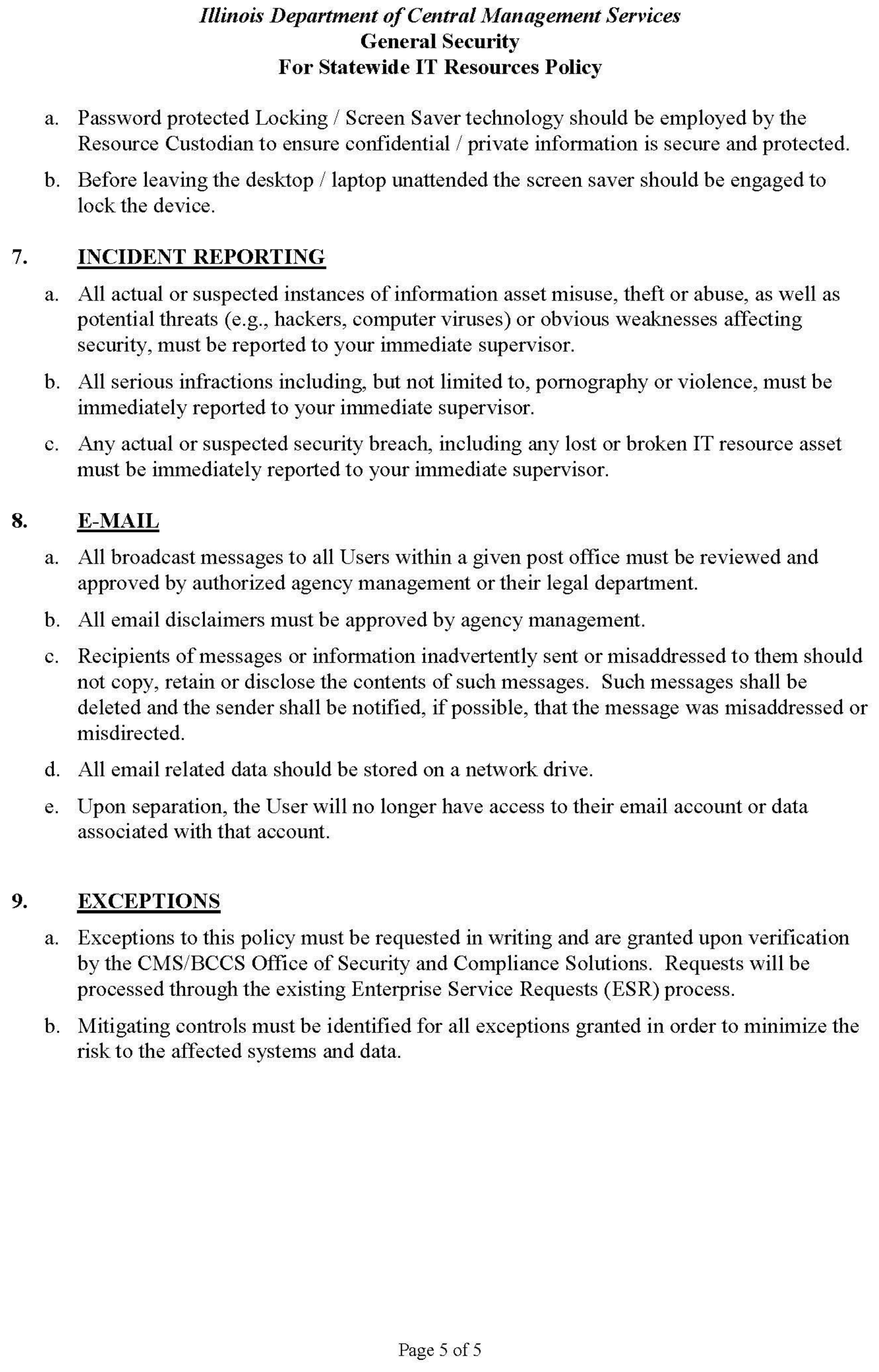
l. Participation in any activity that could potentially cause damage to the image of the State, an agency, or an individual State worker including but not limited to online auctions, personal shopping, private/personal chat room conversations, etc.;

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



Illinois Department of Central Management Services
General Security
For Statewide IT Resources Policy

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.

NOTE: Additional DOIT Policies are on the DOIT Website**. These policies include additional IT Policies, Supporting Definitions, and General Policies.**