Commonwealth Office of Technology
Standard Process

Process Number: COT-067

Effective Date: 02/12/2001
Revision Date: 8/12/2016
Reviewed Date: 6/05/2018

Subject: Enterprise Security Standard Process and Procedures Manual (ESSPPM)

Process: The Enterprise Security Standard Process and Procedures Manual (ESSPPM) has been developed to provide a comprehensive approach to security planning and execution to ensure that Commonwealth managed assets (hardware, software, and data) are afforded appropriate levels of protection against destruction, loss, unauthorized access, unauthorized change, and disruption or denial of service.

Process Maintenance Responsibility: The Office of the Chief Information Security Officer is responsible for maintaining and updating this procedure manual.

Commonwealth Office of Technology

Enterprise Security Standard Process and Procedures Manual (ESSPPM)

TABLE OF CONTENTS

INTRODUCTION

1.0 General

This Enterprise Security Standard Process and Procedure Manual (ESSPPM) has been developed by the Commonwealth of Kentucky's Commonwealth Office of Technology (COT). It contains IT security process and procedures that are to be reviewed and practiced by all Commonwealth Executive Branch staff, including employees, contractors, consultants, temporaries, volunteers, vendors and other worker's. The Commonwealth's Enterprise Information Security Program aligns with the security framework of the current National Institute of Standards and Technology (NIST) Special Publication 800-53. This manual provides guidance for security best practices as they relate to Commonwealth of Kentucky and identifies the specific procedures that staff must follow to comply with enterprise security objectives.

This document has been formatted into sections to ease revision and distribution. The formatting also allows for individual sections to be easily referenced and shared with customers and vendors.

This ESSPPM provides a comprehensive approach to security planning and execution to ensure that enterprise IT assets (hardware, software, and data) are afforded appropriate levels of protection against destruction, loss, unauthorized access, unauthorized change, and disruption or denial of service.

1.1 Objective

The objective of this ESSPPM is to provide a comprehensive set of security processes and procedures detailing the acceptable practices for use of IT assets. The security procedures are set forth to accomplish the following:

- Assure the proper implementation of security controls within the enterprise environment.
- Demonstrate CIO, CISO and Executive Branch management commitment to, and support of, the implementation of security measures.
- Document acceptable practices of enterprise IT equipment and services.
- Achieve consistent and complete security across the Commonwealth's diverse computing environment.

1.2 Scope

The ESSPPM is intended to address a broad range of security related topics and is organized into the following subject areas:

- **Logical Security** -consists of software safeguards for an organization's systems, including user identification and password access, authenticating, access rights and authority levels.
- **Managerial Security** -the identification of an organization's assets (including information assets), followed by the development, documentation, and implementation of policies and procedures for protecting these assets.
- **Physical Security** -the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.
- **Contingency Planning** - a course of action designed to help an organization respond effectively to a significant future event or situation that may or may not happen.

- **Security Awareness Program** -a formal process for educating employees about computer security as well as enterprise policies and procedures for working with information technology (IT).

Within each subject area, specific procedures will be listed and explained.

1.3 Applicability

The security procedures listed within this ESSPPM are applicable to all Executive Branch agencies of the Commonwealth of Kentucky and all staff working on or with enterprise IT equipment or services. Questions concerning the process or procedures described herein should be directed to either the staff's immediate supervisor or to the Office of the Chief Information Security Officer.

SECURITY ORGANIZATION

2.0 Roles and Responsibilities

COT is responsible for providing leadership, policy direction, and technical support to all Executive Branch agencies of the Commonwealth of Kentucky in the application of information technology. This broad statement of responsibility encompasses major information resource functions such as data center operations, communications (voice, data, and video), the use of application development, data administration, hardware selection and installation, and related end user and customer support services.

Individual roles and responsibilities are defined below; however, the following responsibilities are shared by all:

- Participate in information security awareness program activities.
- Report security breaches and violations to the Office of the Chief Information Security Officer (COTSecurityOperations@ky.gov or 502-564-1532).
- Comply with all other Enterprise Security Policies.

2.0.1 Custodians and Data Owners

COT serves as a custodian to the Commonwealth of Kentucky data which is processed and stored on enterprise computer resources that must be protected in accordance with its designated sensitivity and criticality. Data owners provide the management and oversight of agency data assets to help provide business users with high-quality data that is easily accessible in a consistent manner. All data files and applications have an owner. Data owners are primarily Commonwealth of Kentucky agencies, but may be contractors, vendors, government entities, or other authorized users.

Data owners are responsible for:

- Working with COT system administrators, security, and network personnel to ensure access to the data and application(s) is limited to those with a legitimate business need.
- Ensuring that security measures and standards are implemented and enforced in a method consistent with Enterprise Security Policies;
- Establishing measures to ensure the integrity of the data and applications for which COT is the custodian.
- Authorizing appropriate security access levels (read, write, update, etc.) for the data and applications for which COT is the custodian.

- Periodically reviewing access rights to determine the continued need at the level assigned for authorized users.
- Assuring that data is protected at a level required by all applicable regulatory compliance standards.
- Assuring a process is in place to retain or purge information according to record retention schedules as set by the Kentucky Department of Library and Archives (KDLA).
- Determining the classification of data (4080 Data Classification Standard) based on sensitivity, criticality, and application based on established Federal, State, and organizational definitions.

2.1 Authorized Users

Authorized Users are responsible for:

- Understanding and complying with the policies, procedures, and laws related to authorized access to Commonwealth of Kentucky systems and data.
- Informing management when in doubt, about the ethical implications of any given situation or proposed course of action.
- Not subverting or attempting to subvert security measures.
- Reporting any potential violation of these policies to management.

2.2 Management

Managers are responsible for:

- Creating, disseminating, and enforcing conditions of use for facilities and applications under their control.
- Responding to concerns regarding alleged or real violations of this manual.
- Monitoring the use of enterprise resources.
- Taking appropriate disciplinary action for violation of the procedures and/or processes described in this manual.
- Ensuring that staff understands security responsibilities.
- Determining the access requirements of staff, ensuring completion of the appropriate forms, including all required authorizations for the application(s) requested, and maintaining appropriate copies for auditing and historical purposes.
- Communicating both employee and non-employee terminations and status changes immediately to the Commonwealth Service Desk (CommonwealthServiceDesk@ky.gov) so that the appropriate staff are notified to ensure proper deletion/revision of user access.
- Ensuring a secure physical environment for use of enterprise resources.
- Evaluating all security violations reported against staff, contractors and vendors, then taking appropriate action.

2.3 System/Network Administrators

System/Network Administrators are responsible for:

- Taking reasonable action to ensure the authorized use and security of data and communications on systems and networks.
- Responding to questions relating to appropriate use of system and network resources.
- Providing advice regarding the development of conditions of use and authorized use procedures.

LOGICAL SECURITY PROCESSES AND PROCEDURES

All information processed and stored on enterprise computer resources must be protected in accordance with its designated sensitivity and criticality. Logical access controls must be implemented on all enterprise computer systems. Custodians and Data Owners shall be responsible for ensuring that all enterprise computer systems are designed and maintained with the appropriate degree of security necessary to protect computer functions, operations, and resources.

This applies to the implementation of logical security controls in place to protect the Commonwealth of Kentucky data resources and the assets on which they reside.

3.0 Security Software Overview

Systems, network, and software must adhere to the highest level of sensitivity and criticality of the data they process.

All software must be sufficiently protected and monitored to prevent unauthorized use, copying, modification, deletion, destruction, or denial.

Security software must be installed to prevent general users the capability to view password or access control tables, bypass security mechanisms, or use restricted security software functions.

The access privileges to modify software, to use restricted software utility programs, or programs with the diagnostics capable of bypassing or compromising security must be restricted to authorized personnel only. There must be some level of separation of duties prior to releasing code modifications.

3.1 Security Software Design

At a minimum, all security software used to protect Commonwealth of Kentucky information must provide user identification, authentication, data access controls, integrity, and audit controls. Only security software approved by the Kentucky Information Technology Standards may be used for securing Commonwealth of Kentucky information systems.

Security software must be adequately tested to confirm functionality and to ensure that it is minimally disruptive to all associated operating systems, communications, applications, and other associated software systems. Contractual provisions must also ensure that the vendor's software, by design or configuration, will not introduce any security exposures.

Vendor supplied system software (operating system, database management, communications), must be used as the primary source of security features, and supplemented as necessary by customization, to meet or exceed enterprise specifications. Customized and third-party add-on security software shall be used to supplement lack of built-in security features in order to meet security requirements.

The level of protection afforded by security software should be commensurate with the sensitivity of the data. As an example, for data residing in a database that is deemed sensitive or confidential, stringent access controls to the database along with column/row level views should be employed. The level of protection along with the methods to implement that protection should be addressed early in the system development life cycle. Therefore, a task in the Requirements Gathering and Analysis Phase must include consulting with the Office of the Chief Information Security Officer to determine the appropriate levels and methods for data protection. Project plans should document system security requirements that outline planned access, authentication and security controls for the system. The Office of the Chief Information Security Officer will review in a consulting role and make comments and recommendations on the security components.

3.1.1 Software Copyright

Executive Branch staff must comply with national, international, and commercial software license laws along with enterprise security policies and procedures regarding the proper acquisition, use, duplication and distribution of copyrighted software.

COT Asset Management is responsible for periodically reviewing compliance with software licenses and copyright policies. Additionally, management is responsible for ensuring that the necessary documentation is available to provide proof of proper software acquisition.

3.1.2 Software Protection (Malicious Code)

Please review the Enterprise Anti-Virus Policy (CIO-073). A link to this policy is also included in Appendix B.

3.2 Software Development

All software utilized on enterprise computer resources must be designed and maintained with the degree of security necessary to protect sensitive functions, operations, and resources. The level of security protection must be in compliance with the sensitivity of the data. Security and controls are best achieved when they are designed into a system as it is developed. This approach is by far the most cost-effective means of providing security and controls.

Security features necessary for safeguarding information must be included in the design and implementation of applications and systems. Security controls must be documented within a System Security Plan and provided to the Security Office for review and comment. The controls must be approved prior to software development and/or the beginning of installation work. The areas to be reviewed include, but are not limited to, logical security, access controls, system administration, operations security, change management, and disaster recovery/business continuity. Security controls established for each software layer (application, middleware, database, client and server operating system, and network) must be identified. In addition, the confidentiality, integrity and availability of the data must be addressed.

3.2.1 Security in the System Development Life Cycle Process

Retrofitting security into an operational system is difficult, expensive, time consuming and sometimes impossible. Security must be addressed when application systems are being designed, converted, modified, or purchased. Security of applications and software shall be formally addressed, starting in the requirements gathering and analysis phase of the System Development Life Cycle. Security controls must be documented and provided to the Office of the Chief Information Security Officer for review and comment as identified in the prior section.

3.2.2 Software Testing

Software testing for systems that handle sensitive and confidential information must be accomplished with “sanitized” or “masked” production data. Sanitized data is production information which no longer contains specific details that might be valuable, critical, sensitive, or private.

3.2.3 Development Staff Access to Production Application Information

Development staff shall not have access to production data unless approved by the data owner. This access must be documented, and access revoked after the request has been completed. The Security Exemption Request form (COT-F085) must be used to request an exemption. Exemptions should be sent to commonwealthservicedesk@ky.gov . Any access requests for this type of access must include specific details such as type of data, business case for the access and a defined timeframe for which the access is needed.

It is the responsibility of agency management to ensure that separation of duties exists among development staff performing various functions. Control points must be identified to ensure that there is appropriate approvals/sign-offs. For example, a developer that has written and tested code must not be given the access to move that code to production. If development staff is responsible for moving code to production, then different members of the development staff must perform this function. At a minimum, separate directories or libraries with strictly enforced access controls must be employed. Production access must be reviewed on an annual basis to ensure that access is still required.

3.2.4 Software Maintenance with Source Code

All permanent changes to production software must be made with source code rather than with object code or other executable code.

3.3 Restricted Security Activities

Security activities must be strictly controlled to only explicitly identified individuals. Exploitation of security controls and systems security vulnerabilities are examples of restricted work. The following sections identify specific restrictions related to security activities.

3.3.1 Probing/Exploiting Security Controls

Staff are strictly prohibited from probing or trying to subvert security controls unless specifically approved in advance, in writing, by the Chief Information Security Officer. This includes, but is not limited to, the use of both shareware and commercially available scanning software and utilities, vulnerability assessment tools, and denial-of-service utilities. The Security Exemption Request Form (COT-F085) must be used to request an exemption. Exemptions should be sent to commonwealthservicedesk@ky.gov.

3.3.2 Exploiting Systems Security Vulnerabilities

Staff shall not exploit vulnerabilities or deficiencies in information systems security to damage systems/information, to obtain resources beyond those they have been authorized to obtain, to take resources away from other users, or to grant access to systems for which proper authorization has not been granted. All such vulnerabilities must be reported to the Commonwealth Service Desk.

3.3.3 Using Honeypots

The use of honeypots is strictly prohibited. Honeypots are not considered to be a viable intelligence gathering avenue. Honeypot use is illegitimate, accidental or hostile in nature.

3.3.4 Cracking Passwords

Password cracking is prohibited unless specifically approved in advance, in writing, by the Chief Information Security Officer. The Security Exemption Request Form (COT-F085) must be used to request an exemption. Exemptions should be sent to the Commonwealth Service Desk.

3.3.5 Limiting Functionality for Tools

Tools must be used for their intended functionality as opposed to other activities that may cause considerable damage to Commonwealth of Kentucky information resources. For example, network staff may have the need to use hardware/software to sniff the network for troubleshooting activities. Authorization to use this software for troubleshooting activities does not imply that consent has been provided for other activities that could be used to cause significant damage (i.e., collection of critical or sensitive information).

3.3.6 Disabling Critical Components of Security Infrastructure

Critical components of the COT security architecture must not be disabled, bypassed, or turned off without prior approval from the Chief Information Security Officer. Examples could include but not be limited to, firewalls, intrusion detection software, and audit/event logging.

3.4 Change Control Overview

All changes to production computer resources (applications, software, hardware, network infrastructure, etc.), must follow the appropriate enterprise IT Change Control procedures for approval and documentation.

3.5 Software Changes/Configuration Management

The Asset Management Division must maintain an up-to-date inventory of computer software under its control and provide for quality assurance. Configuration records must identify the name, version number, release date, platform, data custodian, and domain/region of all software residing on enterprise computer systems.

Verification must also be performed to confirm the identity of the sender or vendor supplied software. Existence of appropriate contractual agreements for use of vendor software must be confirmed. Contractual provisions must ensure that the suppliers' software by design or configuration will not introduce security exposures.

All computer and communications systems used for production processing at COT must employ a formal change control procedure which is used to ensure that only authorized changes are made and adequately documented. This change control procedure must be used for all significant changes to software, hardware and communications links.

Staff who are primarily responsible for developing and modifying application programs shall not have the ability to move the programs from the testing environment into the production processing environment, thereby circumventing the configuration management process.

3.6 Data/Media Security Overview

All data and media must be sufficiently protected and monitored, consistent with Media Protection Policy, to prevent unauthorized use, modification, disclosure, destruction, and denial of service. Security controls must be applied in a manner that is consistent with the value and classification of the data. Access to data must be granted to users only on a "need-to-know" basis, subject to approval by the designated data owner of the information assets and compliance with policy.

3.7 Data Classification

All Commonwealth data must be appropriately reviewed by the data owner to determine its level of sensitivity and/or criticality. If the environment has a mixed set of classified data, the classification that requires the most stringent controls must be used. Any exception to these standards requires approval by the Chief Information Security Officer. A definition of the COT Data Classification guidelines can be found in the 4080 – Data Classification Standard within the Enterprise Architecture and Kentucky Information Standards Data Domain.

3.8 External Markings

All physical media shall contain external restrictive markings for easy identification as Commonwealth of Kentucky property and the level of data sensitivity. Media belonging to external vendors that is in the care of enterprise staff is subject to the same restrictions.

3.9 Printing/Display

All systems that process, display, or output sensitive must incorporate, and present to the user, an approved banner or notice that addresses the sensitivity of the data and references applicable protection standards. Hardcopy output must be handled in accordance with the Media Protection Policy. Additional labeling requirements may be required based on federal, state, or business compliance needs.

3.9.1 Reproduction

Whenever sensitive cabinet and/or agency documents/media are reproduced in total or in part, the reproductions shall bear the same restrictive legends as the original. Reproductions of sensitive media shall be limited to the minimum number of copies required. All staff must ensure that any sensitive or confidential information that is printed to a central printer is picked up immediately.

3.10 Storage

All media entering or leaving offices, processing areas, or storage facilities must be appropriately controlled. Storage areas and facilities for sensitive media shall be secured and all filing cabinets provided with locking devices appropriate to their sensitivity and protective requirements. Removable media must be stored in a fire-system protected receptacle or off-site storage facility. Storage of all sensitive data must be in compliance with the enterprise Media Protection Policy.

3.11 Disposal/Destruction

All sensitive or confidential information shall be afforded special handling regarding its disposal/destruction. This may include the use of shredders, special burn facilities, or other measures approved in the Media Protection Policy.

3.12 Shredders

Shredder boxes shall be placed adjacent to printers to allow for shredding of confidential information in the event that unnecessary copies are printed.

3.13 Shipping and Manual Handling

Commonwealth of Kentucky information must not be supplied to vendors, contractors or other external organizations without properly executed contracts and confidentiality agreements specifying conditions of use, security requirements, and return dates. When shipping sensitive or confidential information, all available measures must be used to protect the data in transit and actions taken to verify receipt of delivery.

3.14 Facsimile Transmission

Facsimile transmission of sensitive or confidential data shall not occur unless there are exigent circumstances which require this approach. Under no circumstances shall federally regulated data be transmitted via an unsecured facsimile.

If sensitive or confidential information is to be sent by fax, the recipient must first have been notified of the time when it will be transmitted, and also have agreed that an authorized person will be present at the destination machine when the material is sent. An exception will be made if the area surrounding the fax machine is physically restricted such that persons who are not authorized to see the material being faxed may not enter. Individuals may also use fax service where faxes are directed to their inbox, thus providing a higher degree of security.

Sensitive or confidential Commonwealth of Kentucky information must not be faxed via un-trusted intermediaries like hotel staff, rented mailbox store staff, etc.

3.15 Electronic Transmission (E-mail, File Transfer Protocol, etc.)

If sensitive or confidential information is sent via the Internet or other unsecured media transmission facility, the information must be sent encrypted. Current encryption solutions can be located in the Enterprise Standards. The prescribed level of protection will be dependent on the classification of the data to be transmitted. The 4080 – Data Classification Standard should be consulted to determine the appropriate protection profile. In general, all sensitive or confidential data bring transmitted in unencrypted form should utilize end to end encryption. If the data is encrypted appropriate to its classification level, it may be transmitted via unencrypted means.

Federally regulated data shall be encrypted according to the specification dictated by the appropriate legislation.

3.16 Telecommunications Security Overview

All data connections to external computer systems must be protected to ensure that only authorized users and information packets may come in contact with Commonwealth of Kentucky computer systems. The level of filtering, supplemental authentication, audit logging, and associated access restrictions must be based on the risk posed by the attached computer systems and applications on both sides of the network connection. Network connections among systems, including but not limited to links, dial-up access, gateways, bridges, routers, protocol converters, packet assembler/disassemblers, and micro-to-mainframe links must be designed and implemented in a manner to ensure compliance with the appropriate access control for each connected system.

3.17 Remote Access Controls

Remote access controls must be implemented only through approved combinations of hardware and software security tools that meet the specifications of Identity and Access Management Policy and the following requirements:

- Capability to restrict access to specific nodes or network applications
- Access control software/hardware that protects stored data and the security system from tampering
- The access control mechanism must support audit trails of successful and unsuccessful log-in attempts
- Staff must be cognizant of not storing sensitive information (including system passwords) when connecting remotely.

3.17.1 Requesting VPN Access Process

To request VPN access to the Commonwealth-owned electronically-stored data resources the Employee Service Request form (COT-F181 or COT-F181EZ) must be completed and forwarded to the Commonwealth Service Desk. Agencies may have additional internal procedures that are perquisite to this final request to COT, please refer to your agency processes prior to submitting a request for access.

3.18 Remote Network Access Control

It is the responsibility of the Commonwealth Office of Technology (COT) to provide secure and reliable wide-area-network (WAN) and Virtual Private Network (VPN) access for agencies. In order to reduce exposure to security vulnerabilities, all external communications links must be managed outside the state's Intranet in compliance with CIO-074 Enterprise Network Security Architecture.

3.18.1 Encryption

Remote access must be protected by enterprise encryption systems. End-to-end protocol level encryption is the desired method. This encryption should be of industry standard algorithms and key lengths (e.g. AES using a 256-bit key). Reference the Enterprise Architecture and Kentucky Information Technology Standards 5100 – Encryption category within the Security Domain.

3.18.2 Supplemental Encryption

Data that has been identified to be sensitive or confidential in nature by the data custodian shall be encrypted with the aid of authorized encryption programs when stored on disks, tapes, or other media. Consult the Office of the Chief Information Security Officer for authorized processes for a network solution for encryption.

3.18.3 Supplemental Authentication

Some remote access will require enhanced authentication through use of multi-factor authentication technologies such as a onetime use token or hardware key.

3.19 Internet (Firewalls)

All connections between COT **internal** networks and the Internet (or any other publicly-accessible computer network or less restrictive security zone) must coincide with CIO-076 - Firewall and Virtual Private Network Administration Policy. Reference the Enterprise Architecture and Kentucky Information Technology Standards 5700 – Firewall category within the Security Domain.

Only services that are explicitly authorized by the CIO, Deputy CIO and Chief Information Security Officer will be permitted inbound and outbound between COT internal computer networks and the Internet. It is the responsibility of the Office of the Chief Information Security Officer, in conjunction with the appropriate System/Network Administrators, to periodically review the Firewall rule base(s).

Internal network addresses, configuration, and related system design information for enterprise networked computer systems must be restricted such that both systems and users outside the internal network cannot access this information without explicit management approval.

The establishment of a direct, real-time connection between Commonwealth of Kentucky computer systems networks and networks at external organizations such as vendors, via the Internet or any other public network, is prohibited unless the connection has first been approved by the Office of the Chief Information Security Officer. This will allow the Office of the Chief Information Security Officer to document the connection, how the connection will be used, what type of traffic will flow through the connection, determine the anticipated volume, and what specific resources the external entity is required to access so that work with the appropriate Divisions within COT can be performed and appropriate security measures can be implemented (firewalls, routers, etc).

With the exception of dial-up connections, all real-time external connections to Commonwealth of Kentucky internal networks and/or multi-user computer systems must pass through a Firewall-type access control point before users reach a log-in banner. Firewalls provide the ability to log and filter traffic and their audit logs can be used when researching potential security breaches. Dial-up connections shall be enabled on an “as needed” basis only.

3.20 Workstation Security Overview

All workstations equipped with fixed storage devices, e.g., hard disks, shall have security policies established and implemented to restrict unauthorized individuals and applications from accessing information and software stored in the workstation and associated peripherals.

3.21 Mandatory Protection for all Workstations

All workstations shall:

- Have adequate controls to provide continued confidentiality, integrity, and availability of data stored on the system.
- Employ an approved access control mechanism (e.g., software or hardware to restrict access by unauthorized users).
  - Be configured in accordance with CIO-072 Identity and Access Management Policy.

Additional security measures shall stipulate that:

- Critical business functions must not reside on workstations unless specifically authorized for that environment.
- Before leaving their workstations, all staff shall log out, or invoke a password-protected screen saver or session lock. Workstations must employ automated session lock capabilities when left unattended.
- Unless otherwise notified by systems administrators or the Chief Information Security Officer, all staff shall shut down and power off their workstations on Friday afternoon or the end of the employee's work week. Computer monitors should be powered down nightly to conserve energy. Because operating system updates and patches, virus updates, and software implementations and updates are deployed during the work week, workstations should remain powered up on Monday through Thursday evenings.

3.21.1 Protection for Sensitive Workstations

Workstations that access, store sensitive, or confidential data shall have additional password protection, which prevents the rebooting or powering on of the workstation without authentication. Furthermore, workstation equipment must be physically protected to lessen the risks of theft, destruction, and unauthorized access to data. Backup and recovery processes should be considered for these devices.

3.21.2 Resident Protection from Malicious Software

Workstations shall employ approved malicious code screening programs at all times (see CIO-073, "Anti-Virus Policy").

Users shall:

- Immediately notify the Commonwealth Service Desk if a virus is suspected.
- NOT attempt to eradicate a virus.
- NOT use the affected machine until the problem is addressed, documented and resolved.

3.21.3 Erasure of Restricted/Confidential Information

COT or an authorized agency shall electronically erase sensitive data from media or overwrite it with approved software before the media leaves the Commonwealth of Kentucky environment. This does not apply to confidential data written to media as part of scheduled backup processes. Due to the wide availability of programs to restore files that were accidentally deleted, the erasure of sensitive data must be accomplished by means other than deleting the file.

For more information on electronically erasing sensitive data, see Enterprise Policy CIO-092, "Media Protection".

3.21.4 Workstation/Server/Device Equipped with Modems

COT shall approve all network connections for workstations, servers, and devices with modems. Workstation modems and telecommunication lines shall be configured to permit outbound dialing only. Auto-answering modems shall not be used unless approved through the Office of the Chief Information Security Officer.

3.21.5 Unattended Workstation Processing

Some workstations perform specialized monitoring and logging functions and cannot be shut down in any manner. Security measures for these machines shall include, as a minimum, password-protected screensavers, and preventing physical access to the keyboard. Workstations that may not be shutdown should be labeled as such and an appropriate procedure in place to address manual restarts to implement operational changes such as security patching.

3.21.6 Authorized Applications

Only Commonwealth authorized applications and utilities shall be loaded on user workstations. Installing unauthorized applications can impact the performance of the workstation and potentially circumvent security controls. Unauthorized applications will be removed and the user may be subject to disciplinary actions.

3.21.7 Workstations that Employ Password Controls

For workstations that employ operating systems software that have the capability to enact password restrictions that bypass the Enterprise standard authentication controls, those capabilities must be disabled.

3.22 Hardware Authorization

Hardware that is provided by a vendor or contractor to be used on the Commonwealth's network or with any hardware device maintained by the Commonwealth must adhere to the controls set forth for approved Commonwealth hardware and comply with Commonwealth Enterprise Architecture and Kentucky Information Technology Standards. While in use on the Commonwealth network, this hardware will be maintained by COT to ensure compliance. This hardware must be inspected and approved for use by the appropriate COT team prior to being placed on the network. COT personnel will ensure that this hardware is free of any viruses and malware and that enterprise standard anti-virus software has been installed, pursuant to CIO-073, "Anti-Virus Policy". In addition, COT personnel will ensure that any agents required for updates to software and operating systems have been installed and all relevant operating system patches and software updates have been applied. When this hardware will no longer be used on the Commonwealth network, any COT licensed software must be completely removed. Personally owed hardware must not be connected to any state asset or network.

MANAGERIAL SECURITY PROCESSES AND PROCEDURES:

The protection of Commonwealth of Kentucky information resources is a basic responsibility of management. Each manager is responsible for security within their area of control. They are also responsible for ensuring all staff know and understand their obligations to protect information resources. Therefore, each manager must ensure that security implementing procedures and practices are promulgated and enforced.

4.0 Administrative Security Overview

All operating systems, communications software, program products, security software, applications, and data must be sufficiently protected and monitored, consistent with enterprise IT security policies, to prevent unauthorized use, modification, disclosure, destruction, and denial of access.

4.1 Access Control and Accountability

Access control and accountability are configured in accordance with the Identity and Access Management Policy (CIO-072). A link to this policy is also included in Appendix B.

4.1.1 Individual Access Authorization for Employees

Authorization for individual access must be based on a documented request that identifies resources required. The request must be submitted to the Commonwealth Service Desk by the user's manager, who must educate the user on computing asset responsibilities. The "Employee Service Request Form" (COT-F181) is used to request access to COT-controlled servers and network. The documented request must be retained for a period of time as identified by KDLA record retention policies. As part of entrance procedures, all new staff are required to sign the "Acknowledgement of Responsibility Form"; COT staff are required to sign COT's Acknowledgement of Responsibility form, (COT-F015). The form acknowledges responsibilities pertaining to confidentiality and integrity of data, policies and procedures, and proper use of resources. The "Acknowledgement of Responsibility Form" (COT-F015) must be electronically signed on an annual basis by all employees to ensure that responsibility is understood. Agencies must implement similar acknowledgements to ensure that employees are aware of their role in the protection of Commonwealth data and resources.

4.1.2 Individual Access Authorization for Contractors

Prior to employment, contractors desiring to work for COT shall be screened thoroughly and their qualifications verified. Contractors hired to work for COT shall be required to sign the "Acknowledgement of Confidentiality Agreement Form", (COT-F011). The "Acknowledgement of Confidentiality Agreement Form" must be electronically signed on an annual basis by all contractors to ensure that responsibility is understood. Agencies must implement similar acknowledgements to ensure that employees are aware of their role in the protection of Commonwealth data and resources.

4.1.3 Individual Access Termination

Access privileges must be terminated immediately when a user's authorization ceases as identified by the user's manager. When staff transfer, resign or have their employment terminated, their manager is responsible for completing all required paperwork such as "Employee Service Request form" (COT-F181) to remove all access and privileges of the departing employee. For situations involving termination, the Office of the Chief Information Security Officer must be notified immediately so UserIDs assigned to the individual may be disabled, minimizing the security exposures a potentially disgruntled individual may cause. The manager must reclaim the badge and properly dispose of the badge.

4.1.4 Monitoring of Email

An agency may request a review of staff members' e-mail account(s) when circumstances warrant (investigating potential risk situations, appropriate use of email, etc.) The agency should consult Enterprise Policy CIO-084, "E-mail Review Request" for complete details.

4.1.5 Communication Link Control

An unauthorized communication link may compromise the security of computing assets. Control of communication links to a computing asset is necessary to ensure that no covert channels are permitted. The Owner must control those links for which they are responsible. Any unauthorized communication link identified will be subject to immediate termination and blocking.

4.1.6 Dial-Up Access Control

Dial-up access to Commonwealth of Kentucky computing assets must be controlled so that the identity of the caller is verified before access is granted. The connection between the dial-up device and the computing asset must meet the requirement of communication link control. Dial-Up connections must only be enabled on an as needed basis.

4.2 Host Environment

Baseline configurations and set-up parameters on all hosts attached to the enterprise network must comply with security management policies and standards. Management must ensure that system owners and support teams document and maintain security baseline configurations for supported platforms and keep them current based on annual reviews.

4.3 Network Environment

This section describes managerial processes specific to the Network Environment (Local Area Network).

4.3.1 Access to Shared File Storage Areas (Directories)

While it is recognized that shared file directories are necessary to facilitate individuals getting their work completed. It's a common business practice that shared file directories are established along branch and other organizational boundaries. If shared files have been restricted, access will be granted by authorization level. The following shared file directory authorization scheme will be observed:

- The CIO will have the right to access all files under their area of responsibility.
- The Director will have the right to access files under their area of supervision.
- The Branch Manager will have the right to access files under their area of supervision.
- An individual section will have access to its individual files or other files as authorized by the branch manager.

4.3.2 Supervisor Capabilities

Only those individuals designated as System/Network Administrators will have Supervisor capabilities to the servers for which they are responsible. Furthermore, the Supervisors must adhere to the processes set forth in this document and other enterprise security documentation when administering and configuring Commonwealth of Kentucky servers.

4.3.3 Security Privileges

The least amount of security privileges required for a person, process, or application to perform their job must be assigned. Privileges must be layered to reflect job functions and separation of duties. For example, different security privileges for System Administrators, Backup Operators, Managers and end-users must be defined. A person may be assigned multiple UserIDs in order for them to perform their job duties.

To protect processes and data from faults and malicious behavior, the process of least-privileged user accounts (LUA) should be applied. Any process that requires administrative level access must be executed by an account other than a standard user account. A person requiring administrative-level access to a system, process, or application shall be issued a separate UserID for these administrative functions in accordance with the Identity and Access Management Policy (CIO-072).

4.5 Procedural Security Overview

Management shall procedurally enforce and monitor access and authorization restrictions to all sensitive information processed or stored within their area. Procedures shall be developed and implemented establishing controls at the points in the work flow where restricted or confidential processing is performed or where control passes from one function, element or individual to another. The procedures shall provide the degree of security determined by management to be necessary for that activity.

4.6 Output Distribution Controls

Management shall heighten the awareness of staff to ensure sensitive or confidential computer generated output must be personally delivered to the designated recipients and must not be delivered to an unattended desk, or left out in the open in an unoccupied office.

4.7 Audit Capabilities

Management shall ensure that security software features must be used to automatically generate and store security audit log records for use in monitoring security-related events on all multi-user systems. The granularity and level of auditing should be commensurate with the sensitivity or confidentiality of the data.

4.7.1 Audit Trails

As a best practice logical audit trail, all log-in and log-in attempts, and unsuccessful computing asset access attempts must be recorded with the following information:

- Logical and hardware source addresses (TCP/IP, MAC, etc.)
- UserID
- Date and time of occurrence
- The activity generating the log event

If there are instances where all log-in activity cannot be recorded due to system constraints, notification shall be provided to the Chief Information Security Officer. The Security Exemption Request form (COT-F085) must be used to request an exemption.

All audit trail records must be:

- Protected from unauthorized access, modification, or destruction.
- Reviewed at least weekly to confirm that there have been no attempted violations.
- Retained for a period of time as determined by the Kentucky Department for Libraries and Archives (KDLA) or federal retention requirement.

To provide a physical audit trail, records of changes to the hardware and software inventory must be maintained by the individual responsible for the inventory. Physical audit trails must record the:

- Identification of person maintaining or removing the computing asset.
- Date and time of maintenance event or removal.
- Identification of computing asset maintained or removed.
- Date and time when computing asset was returned.
- Inspection and acceptance of returned computing asset.

4.7.2 Investigative Support

As a best practice for systems that process sensitive or confidential information, the capability must exist for recording a session log and for selectively signaling user activity in real time (e.g., a console alarm or other real-time notification of log-in.) This provides the ability to notify the appropriate individuals (Chief Information Security Officer, LAN network administrator, law enforcement authorities, etc.) to track suspect activity in response to a security incident.

4.7.3 Review/Retention Schedule

Audit logs are important for error correction, forensic auditing, security breach recovery, and related efforts. Audit logs containing computer security relevant events must be retained for a period of time as defined by KDLA or any federal requirements. During this period, the audit logs must be secured such that they cannot be modified and can be read only by authorized persons.

4.8 Security Incidents

It is management's responsibility to make sure all staff are trained and aware of how to report suspected security violations properly to the Commonwealth Service Desk (502 564-7576). A security incident is defined to be any event or threat of an event, affecting normal operation of an enterprise managed computer system and/or facility.

Security breaches may be categorized as those pertaining to physical intrusions and electronic intrusions that include network, servers, and workstations. Please reference CIO-092 Incident Response Policy for instructions on reporting.

4.8.1 Additional Requirements for Specific Categories of Security Violations

- For intrusion of secured areas, notification may also include the FBI, U.S. Attorney's Office, Kentucky State Police, local police department, and/or other law enforcement agencies at the discretion of agency executive management.
- For catastrophic disasters such as fire, bomb threats, floods, or destructive storms, notification procedures will include the local fire department and/or police department at the discretion of agency executive management. Staff should be familiar with agency emergency procedures.
- For incidents involving electronic intrusions, other state agencies will be notified as appropriate. Any data captured that resulted in detecting the intrusion should be kept until the incident has been investigated and cleared.
- For incidents involving deception and fraud, additional notification may include the police department depending upon the severity of the incident at the discretion of agency executive management.

4.8.2 Security Incident Handling Guidelines

- Please review Agency Incident Response Guidelines.

4.9 Risk Management and Security Alerts

A formal review of the enterprise computer processing environment shall be periodically conducted to ascertain the effectiveness of the installed security control measures, identify weaknesses, and recommend controls to strengthen the areas where weaknesses are found.

The Office of the Chief Information Security Officer and the System/Network Administrators who are responsible for implementing security measures must stay abreast of security alerts issued by various security organizations and vendors. It is the responsibility of the system/network administrators to promptly review security alerts as identified by the Office of the Chief Information Security Officer. Security patch software must be applied promptly whenever possible. Security alerts shall be made available on the COT website.

4.10 Personnel Security

Standards shall be established to enhance enterprise personnel management practices by prescribing security requirements for personnel assigned to information technology positions. Background checks shall be performed on all current and prospective enterprise staff. Background checks should be conducted periodically, not to exceed every 2 years, to ensure that any changes in personnel risk are identified.

4.11 Privacy

All messages sent over enterprise computer and communications systems are the property of the Commonwealth of Kentucky. To properly maintain and manage this property, management reserves the right to examine all data stored in or transmitted by these systems. In accordance with the Federal Electronic Communications Privacy Act of 1986, employers can monitor electronic messages upon notification. Employees should have no expectation of privacy associated with the information they store in or send through these systems.

In accordance with CIO-060, at any time and without prior notice, Commonwealth of Kentucky management reserves the right to examine archived electronic mail, file directories, hard disk drive files, and other information stored on enterprise information systems. This examination is performed to assure compliance with internal policies, support the performance of internal investigations, and assist with the management of enterprise information systems.

Individuals may be subject to electronic monitoring while on enterprise premises. This monitoring is used to measure workers performance as well as to protect worker personal safety, and enterprise property. In areas where there is a reasonable expectation of privacy, such as bathrooms, dressing rooms, and locker rooms, no electronic monitoring will be performed.

PHYSICAL SECURITY PROCESS AND PROCEDURE:

A balanced information security program must include a solid physical security and environmental security foundation. The establishment of adequate physical access and environmental controls is a necessary and important step in achieving a safe and secure processing environment.

5.0 Physical Access Overview

All state information processing areas must be protected by physical controls appropriate to the size and complexity of the operations and the criticality or sensitivity of the systems operated at those locations. Physical access to areas must be restricted only to authorized personnel. It is the responsibility of each Branch Manager, Director and Executive Director to ensure that all employees abide by the standard procedure concerning physical access.

5.1 Process to obtain badge access

Please follow agency specific guidelines for obtaining physical badge access.

5.2 Restricted Access to the Commonwealth Data Center (Cold Harbor)

Please refer to CIO-058 - IT Equipment Room Access at the Commonwealth Data Center Policy. This policy describes the responsibilities and procedures to be followed when requesting access to IT equipment room areas at the Commonwealth Data Center. Also CIO-059 - Equipment Installation and Removal at the Commonwealth Data Centers Policy outlines the responsibilities and procedures to be followed when equipment is installed in or removed from the Commonwealth Data Centers.

Restricted Areas include but are not limited to the following areas of the Commonwealth Data Center:

- 3rd and 4th Floor
- East/West Warehouse
- Electrical and Maintenance Closets
- Basement Level Mechanical Room

5.3 Badge Auditing of the Commonwealth Data Center (CDC)

In order to ensure badge access is still required, a monthly review of access should be conducted by the appointed authority to determine if access is still needed.

If no access has been made within 90 days, a list should be generated and submitted to an agency point of contact for review. Once approved those persons' badge access will be disabled and their supervisor informed of the change.

5.4 Visitors to the Commonwealth Data Center (CDC)

All visitors to the CDC must adhere to CIO-058: IT Equipment Room Access at the Commonwealth Data Center

5.5 Visitor Logs for the Commonwealth Data Center (CDC)

In order to maintain accurate records on visitors, a visitor log must be maintained at the Commonwealth Data Center. Procedures for visitor logs are as follows:

- Visitor logs should be maintained in chronological order.
- Logs will be retained for a period of time as defined by KDLA or any other local, state, or federal requirements.
- Logs should also include entries from employees that are visiting the building from other offices if the employee's badge does not automatically provide access.

5.6 Facility Construction (Environmental Controls)

Adequate security measures must be in place to protect computer and communications equipment and data from physical damage resulting from power loss/surges, electrostatic discharge, magnetic fields, flooding, fire, smoke, overheating, and other forms of physical threats.

5.6.1 Electrical

The most frequent cause of major computer component failures is power failures. These failures include complete loss of power, brownouts, blackouts, and voltage spikes. To properly protect equipment, all critical hardware must be protected from electrical failures. This includes, but is not limited to, generators and uninterruptible power supplies.

5.6.2 Heat

Sustained high temperatures will cause electronic and mechanical components to prematurely malfunction or fail completely. Overheating is often caused by the obstruction of ventilating grilles. Therefore, adequate, reliable and properly installed air conditioning must be provided and care taken not to obstruct ventilation of major hardware components.

5.6.3 Humidity

The proper humidity levels for critical equipment, as specified by the manufacturer, must be maintained. Low humidity permits the buildup of static electricity charges that may damage electrical components. High humidity, on the other hand, may lead to condensation that causes shorts in electrical circuits and corrosion.

5.6.4 Water

Critical equipment must not be placed directly under water pipes, sprinklers or in areas prone to flooding. Water introduced by rain, bursting pipes and overhead sprinklers has been responsible for more actual computer damage than fire. Detection mechanisms must be in place and monitored for the presence of water in areas housing critical assets.

5.6.5 Dirt and Dust

All air intakes must be filtered and filters must be kept clean. Foreign matter can interfere with the proper operation of magnetic tape and disk drives, printers, and other electronic and mechanical devices.

5.7 Hardware Accountability

Adequate security measures must be in place to protect COT computer and communications equipment and data from physical damage, theft, vandalism, and other forms of physical threats. By maintaining accurate accountability of property and instituting appropriate countermeasures to safeguard property, the opportunity for loss, theft, or pilferage of valuable computer resources can be greatly diminished.

Computing hardware and media must be physically protected against theft, damage (e.g., environmental), and misuse. To satisfy this requirement, the following must be provided:

5.7.1 Inventory

A current record must be maintained of the physical components of the computing asset or group of assets. This record must not be maintained with the assets.

5.7.2 Rooms and Cabinets to Protect Equipment

Rooms intended to provide hardware security must accomplish the following:

- Limit physical access control of equipment configuration.
- Protect hardware from environmental hazards.

5.7.3 Workstation and Terminal Control

Devices outside computer or communications rooms must be:

- Locked, logged off, or physically secured when unattended.
- Housed in a facility that provides adequate protection from theft or provided with additional physical safeguards.
- Protected from environmental hazards (e.g., extreme temperature changes, electrical power surges, dust, dirt, and liquids).

5.7.4 Access Key Control

When access keys or combinations are used, an individual must be designated as responsible for managing, issuing, and recording their distribution. Procedures must be implemented that address the changing of keys or combination in the event of staffing changes.

5.7.5 Portable Equipment Control

Staff that receives permission to remove equipment must provide a reasonable level of protection for that equipment and associated software, data, and media from theft and damage. A record of portable equipment assigned to employees and contractors must be maintained by the individual or group authorized to distribute the equipment

5.7.6 Hardware Changes/Configuration Management

All computer and communications systems used for production processing at COT must employ a formal change control procedure to ensure that only authorized changes are made. Please refer to CIO-101 – Enterprise Release Management Policy. This policy describes the responsibilities and procedures to be followed when making modifications to the Commonwealth of Kentucky's production software applications.

The Change Management Standard Procedure, (COT-009), must be followed to document all significant changes to software, hardware, communications links, and operational procedures.

5.7.7 Theft Protection

To minimize the risk of theft to equipment such as workstations, communications gear, laptops, etc., adequate deterrents such as locked rooms and storage areas, controlled access rooms, and the monitoring of visitors to sensitive information must be performed. Staff in possession of laptops and other transportable computers containing sensitive or confidential Commonwealth of Kentucky information must not check these computers into airline luggage systems. These computers must remain in the possession of the traveler as hand luggage. All portable computing devices must be protected at all times. When stored they must be kept in a locked and secured area outside of the public view. For example, laptops in vehicles should be stowed in non-visible locked locations such as the vehicle trunk.

Whenever equipment containing sensitive or confidential information is removed or relocated, a record of the date, the information/equipment involved, and the persons possessing the information/equipment must be documented and kept with the staff member's Branch Manager. The theft of the equipment itself may result in a loss of several thousand dollars, the theft and disclosure of sensitive information like citizen addresses, social security numbers, etc. could cause considerable risk for the private citizen and potential legal ramifications to the Commonwealth of Kentucky.

CONTINGENCY PLANNING PROCESS AND PROCEDURE

All computer and network resources considered critical to enterprise operations shall have recovery capabilities defined, that will minimize the impact of their disruption or unavailability for whatever cause. Contingency planning is a responsibility of all elements of enterprise. These contingency plans shall provide for resumption of data processing services necessary to ensure an acceptable level of enterprise operations can be maintained. It is prudent and required by enterprise to anticipate and prepare for the loss of information processing capabilities. The plans and actions to recover from losses range from routine backup of data and software in the event of minor losses or temporary outages, to comprehensive disaster recovery and business continuity planning in the preparation for catastrophic losses of information resources.

6.0 Backup Procedures Overview

An integral component in an effective contingency plan is the regular on- and off-site backup of all critical applications, software, documentation, and data files for all of the processing platforms. To minimize the possible disruption to business operations which an incident resulting in loss of data could entail, COT shall establish and maintain an effective schedule for the backup of critical computer and network resources and for the prompt recovery of services following unanticipated interruptions.

6.1 Data Backup

On-site backup is employed to have current data readily available in machine-readable form in the production area in the event operating data is lost, damaged, or corrupted and to avoid having to reenter the data from source material. Off-site backup or storage embodies the same principle but is designed for longer term protection in a more sterile environment, requires less frequent updating, and provides an additional protection against threats potentially damaging to the primary site and data.

Data and software essential to the continued operation of critical department functions must be backed up. The security controls over the backup resources must be as stringent as the protection required of the primary resources. Furthermore, backups should be augmented by using backup generations (e.g., if a full volume backup is performed every night, the previous seven generations may be kept before being over written) and identifying a frequency which backups will be performed.

6.2 Alternate Data Backup

The backup procedures on multi-user computer systems and departmental servers are designed to protect against data losses caused by hardware failures and other disasters. The frequency and timing of these backups may not provide sufficient protection to meet end-user requirements for data backup. To minimize the potential impact a contingency situation impacting the CDC building may have, critical backups must also be kept at off-site storage facilities and must be incorporated into enterprise offsite storage rotation.

6.3 Emergency Response/Recovery Procedures

Each multi-user system must have a designated individual to maintain an up-to-date, documented plan containing emergency response/recovery procedures for recovering the system in the event of a system failure or damage to the facility. Critical systems, pre-requisite jobs, applications and equipment must be identified and prioritized for recovery from outages of different degrees of severity including the established cyclical processing deadlines. Ideally, as a step in the systems development lifecycle, recovery requirements must be defined and addressed.

Contingency plans, or disaster control plans, specify actions management has approved in advance to achieve each of three objectives: to identify and respond to disasters; to protect personnel and systems; and to limit damage. In addition, these plans document how the Commonwealth of Kentucky will respond to contingency situations, responsibilities of individuals, recovery options (hot-site, cold-site, server mirroring, etc.) to be used and recovery priority of business functions and applications.

6.4 Contingency Plan Maintenance and Exercising

The review and maintenance of contingency plans for critical systems and applications must be performed annually or when significant changes have occurred. The data custodian is responsible for all infrastructure components and the data owner will maintain all business functions despite a disruption, compromise, or failure. The exercising of contingency plans for critical systems and applications must be performed at least semi-annually with participation from both parties. Results of these exercises must be adequately documented for subsequent review by management and auditors. It is through exercises, both table-top (walk through) and operational, that deficiencies can be identified and addressed.

SECURITY AWARENESS PROGRAM PROCESS AND PROCEDURE

This section defines and details the requirement and required elements of security education that data custodians are expected to implement to safeguard their computing asset or group of assets. Users must be briefed on their responsibilities for computing security before initial access is given to any enterprise computing asset. Users must also be educated annually on their security responsibilities. To satisfy this requirement, the following must be provided:

- Initial briefing at the time of hire or transfer
- Annual education
- A record of completion of awareness activities.

This applies to all computer and network resources housed and maintained by COT.

7.0 Establishing a Security Awareness Program

The Office of the Chief Information Security Officer and management will meet periodically to:

- Review the current status of enterprise information security policies, procedures and program.
- Review and monitor security incidents that may have occurred within COT.
- Approve and review information security projects.
- Approve new or modified information security policies.
- Perform other necessary high-level information security management activities.

7.1 Security Awareness Training

Security Awareness Training should be completed annually. All employees and contractors must be provided with sufficient training and supporting reference materials to allow them to properly protect the enterprise information resources. They must read and acknowledge their understanding of the contents of enterprise policies and procedures before being granted access to the enterprise computing assets.

All new staff must attend the orientation provided by the Office of Human Resources Management and Development. Security training is included in the initial training for all staff. In addition, all new staff shall be provided with hard copies of security information covered in orientation.

Appendix A – Kentucky Computer Crime Law

Kentucky Computer Crime Law

During the 2002 regular session, House Bill 193 was passed that amended the Kentucky Computer Crime Law (KRS 434.840-855) effective July 15, 2002. The changes are as follows:

- Amends various definitions
- Requires that a person must act without the effective consent of the owner to be guilty of unlawful access to a computer
- Increases penalty for unlawful access to a computer in the second degree to a Class D felony
- Creates two new sections of KRS Chapter 434 establishing crimes of unlawful access to a computer in the third and fourth degrees and establishes a range of penalties

The following links provide the revised statutes:

- KRS 434.840 Definitions:
  http://www.lrc.state.ky.us/KRS/434-00/840.PDF

- KRS 434.845 Unlawful Access to a Computer in the First Degree:
  http://www.lrc.state.ky.us/KRS/434-00/845.PDF

- KRS 434.850 Unlawful Access to a Computer in the Second Degree:
  http://www.lrc.state.ky.us/KRS/434-00/850.PDF

- KRS 434.851 Unlawful Access in the Third Degree:
  http://www.lrc.state.ky.us/KRS/434-00/851.PDF

- KRS 434.853 Unlawful Access in the Fourth Degree:
  http://www.lrc.state.ky.us/KRS/434-00/853.PDF

- KRS 434.860 Misuse of Computer Information:
  http://www.lrc.state.ky.us/KRS/434-00/855.PDF

Appendix B – Commonwealth of Kentucky Enterprise Security Policies

Commonwealth Of Kentucky Enterprise Security Policies
http://technology.ky.gov/policy/Pages/policies.aspx

Agency Incident Response Guidelines
https://gotsource.ky.gov/docushare/dsweb/Get/Document-392942/