Education and Workforce Development Cabinet
Laptop POLICY/PROCEDURE

Policy Number: EDU-08

Effective Date: November 30, 2006
Revision Date: December 20, 2012

Subject: Laptop Policy

Policy: This policy supports the Education and Workforce Development Cabinet (EDU) laptop and mobile computing devices.

Scope: This policy applies to all EDU employees and contractors, including all persons providing contractor services, who use, process, or store computerized data relevant to agency business on an EDU maintained server or workstation.

Policy/Procedure Maintenance Responsibility: The EDU Agency Security Contacts (ASC) is responsible for the maintenance of this policy. The Chief Information Officer (CIO) is responsible for the revision of the EDU Policy and Procedures Manual (PPM). The EDU CIO is responsible for authorizing all changes to the PPM.

Applicability: All EDU employees and contractors shall adhere to the following policy.

Responsibility for Compliance

Each Department is responsible for assuring that employees within their organizational authority have been made aware of the provisions of this policy, that compliance by the employee is expected, intentional misuse and/or inappropriate use may result in disciplinary action pursuant to KRS 18A up to and including dismissal. It is also each Department's responsibility to enforce and manage this policy.

Overview

Description: All laptops acquired for or on behalf of EDU shall be deemed State property. Each employee issued with a laptop is responsible for the security of that laptop, regardless of whether the laptop is used in the office, at the employee's place of residence, or in any other location such as a hotel, conference room, car or airport.

Purpose/Rationale: Set security provisions for securing laptop computers.

Applicability: All individuals assigned laptops and access to the network including but not limited to full and part time employees, temporary workers, volunteers, contractors, and those employed by others to do Education Cabinet work, are covered by this policy and shall comply with this and associated policies, procedures and guidelines.

Failure to Comply: Failure to comply with information security policies or associated polices, standards, guidelines and procedures may result in disciplinary actions up to and including termination of employment for employees or termination of contracts for volunteers, contractors consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Policy

General

a. Division of Technology Services (DTS) will ensure reasonable physical safeguards to maintain laptop computers in such a way to avoid inadvertent disclosure of EDU's information
b. DTS shall be responsible for secure installations, configurations, distribution, management and removal from service, of EDU laptop computers. DTS must document if these responsibilities are assigned to another program area or office.

Securing Laptop Computers

Individuals granted access to the State network or information systems shall secure laptop computers from inadvertent or unauthorized access.

a. When leaving a laptop computer unattended, users shall apply the "Lock Workstation" feature (ctrl/alt/delete).
b. Unattended laptop computers shall be secured from viewing by password protected screen savers and set to activate the automatic screensaver feature after a period of non-use. The period of non-use shall be for no more than ten (10) minutes.
c. Laptop computers shall store confidential and sensitive information on a networked drive (shared directory on the EDU network) and not the user's hard drive. If business requires confidential or sensitive information be available when mobile take only those files that are essential and store as little valuable data on the laptop as possible.

d. Laptops with wireless capability enabled will have VPN software installed. Confidential and sensitive information will be available thru VPN when kept on a networked drive as described in C above.
e. Laptop computers must have firewall software installed and operational.
f. Laptop computers must have antivirus software installed and operational.
g. Laptop computer user shall not permanently disable or alter security safeguard, such as virus detection software, firewall or encryption software installed on the EDU laptop computer.
h. Users are responsible for making sure the Operating System Updates and Virus protection updates are current.
    a. Failure to keep these safeguards current may result in the loss of laptop usage.

Physical Security Measures

Physical security of that laptop, regardless of whether the laptop is used in the office, at the employee's place of residence, or in any other location such as a hotel, conference room, car or airport.

a. Laptop computers actively connected to the network or information systems must not be left unattended.
b. Keep laptop computers out of sight when not in use, employees must avoid leaving their laptop unattended in a public place, if in an automobile lock in trunk, if in a location such as hotel or airport the laptop must either remain with the person or locked in a safe or locker. Laptops that are taken out of the office and will not be used for several days or longer must be locked out of sight in a secure cabinet or safe.

Unauthorized Software

a. Individual users shall not install or download software applications and/or executable files to any EDU laptop computer without prior authorization from DTS.

Viruses

a. Laptop computer users shall not write, compile, copy, knowingly propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer system (e.g. virus, worm, Trojan horse or the like).
b. Suspected viruses should be reported immediately to the Help Desk.

c. Viruses shall not be deleted without expert assistance unless instructed by DTS.

Monitoring of the laptop computers.

a. EDU reserves the right to monitor individual user laptop computers at random and/or for cause.

Technical Security

Laptop computers shall be configured to reduce the risk if inadvertent or unauthorized access to EDU information and systems.

a. All EDU laptop computers shall be configured according to DTS laptop configuration standards.
b. User identification (name) and authentication (password) shall be required to access the operating system of all laptop computers whenever turned on or booted.
c. Local hard drives shall not be accessible when a laptop computer is booted from mobile media, e.g., a diskette, compact disk or USB device.
d. Laptop computers shall be configured to log all significant computer security relevant events, (e.g., password guess, unauthorized access attempts or modifications to applications or systems software.)

Policy exceptions

a. The Security Audit Group shall approve or deny policy exceptions. Policy exception requests shall be submitted electronically or in hard copy for to Security Audit Group.

Review Cycle:

Annually

Timeline:

Review Date: November 29, 2012
Reviewed By: EDU Agency Security Contacts

Enterprise Security and Policies

Cross Reference:
Cross Reference: http://technology.ky.gov/governance/Pages/policies.aspx
CIO-060 -- Internet and Email Acceptable Usage Policy
CIO-073 -- Anti-Virus Policy

CIO-081 -- Securing Unattended Workstation Policy

OTS Standards
Cross Reference:
EDU-01 -- Internet and Email Acceptable Usage
EDU-07 -- Unattended Workstation
EDU-11 -- Anti-Virus
EDU-12 -- Network Services – Data Storage
EDU-F03 -- Security Request Change Request Form