Education and Workforce Development Cabinet
POLICY/PROCEDURE

Policy Number: EDU-17

Effective Date: June 1, 2007
Revision Date: December 20, 2012

Subject: Remote Access Policy

Policy: This policy supports the Education and Workforce Development Cabinet (EDU) regarding Remote Access connections.

Scope: This policy applies to all EDU's employees, contractors, vendors and agents with a state owned or personally owned computer or workstation used to connect to the EDU's network. This policy applies to remote access connections used to do work on behalf of EDU, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in, wireless LAN, modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

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.

Purpose

The purpose of this policy is to define standards for connecting to EDU's network from any host. These standards are designed to minimize the potential exposure to EDU from damages, which may result from unauthorized use of EDU's resources. Damages include the loss of sensitive or company confidential data,

intellectual property, damage to public image, damage to critical EDU's internal systems, etc.

General

1. It is the responsibility of EDU employees, contractors, vendors and agents with remote access privileges to EDU's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to EDU.
2. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of EDU's network:
   a. *Internet and Email Usage*
   b. *User ID and Password*
   c. *Digital Data Storage-Transport*
   d. *Anti-Virus*

Requirements

1. All computers with remote access capability must utilize a state-approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic.

2. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the User ID and Password Policy.

3. At no time should any EDU employee provide his or her login or email password to anyone.

4. Use of remote access controlling software for controlling computers within the EDU must be approved.

   a. Unapproved remote capable software specifically includes NetMeeting, Dameware, trial versions and unlicensed copies of any remote capable software.

5. All hosts that are connected to EDU's internal networks via remote access technologies must use the most up-to-date anti-virus software and operating

system must have all critical updates applied, this includes personal computers.

    a. Users are responsible for making sure the Operating System Updates and Virus protection updates are current on state owned equipment.

Failure to meet these requirements and keep the safeguards current may result in the loss of remote access capability.

Review Cycle:
Annually

Timeline:
Review Date: November 26, 2012
Reviewed by: EDU Agency Security Contacts

Enterprise Security and Policies
Cross Reference:
http://technology.ky.gov/governance/Pages/policies.aspx
CIO-060 -- Internet and Electronic Mail Acceptable Use Policy
CIO-072 -- UserID and Password Policy
CIO-073 -- Anti-Virus Policy

OTS Standards
Cross Reference:
EDU-01 -- Internet and Email Usage
EDU-02 -- User ID and Password
EDU-13 -- Digital Data Storage-Transport
EDU-11 -- Anti-Virus