

**Education and Workforce Development Cabinet
POLICY/PROCEDURE**

Effective Date: March 1, 2007
Revision Date: February 12, 2007

Subject: Bluetooth Technology, Infrared Technology

Policy: This policy supports the Education and Workforce Development Cabinet (EDU) regarding Bluetooth Technologies.

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 Security Audit Group (SAG) 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).

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

Bluetooth and Infrared enabled devices are becoming more prevalent in the computing environment and pose security risks. Due to the vulnerabilities in the Bluetooth and Infrared technologies will not be supported.

Purpose/Rationale: Bluetooth and Infrared enabled devices are vulnerable to multiple attacks. Due to the security risk on data, no Bluetooth or Infrared device will be connected or interact directly with the network.

Applicability: All laptops, PDA (Personal Digital Assistant) or any device directly connected or interacting with the network shall have the Bluetooth or Infrared Technology disabled.

Blackberries and cell phones can use the Bluetooth and Infrared Technology for headset,

keyboard usage but will be specifically denied from interacting with the network.

Review Cycle:

Annually

Timeline:

Revision Date: February 12, 2007

Review Date: November 30, 2011

Effective Date: March 1, 2007

Enterprise Security and Policies

Cross Reference: <http://technology.ky.gov/governance/Pages/policies.aspx>

CIO-071 Wireless Voice and Data Services Policy

DTS Standards

Cross Reference:

EDU-08 Laptop Policy

EDU-15 Wireless Voice and Data Services Policy