EDUCATION and Workforce Development CABINET
POLICY/PROCEDURE

Policy Number: EDU-09 **Effective Date**: 04/01/04
Revision Date: 01/20/05

Subject: Logon Security Notice

Policy Statement: This policy is intended to protect the confidentiality, availability, and integrity of the Commonwealth's information technology resources, by requiring all logon screens include a security notice indicating that the system must be used for authorized purposes only. A security notice or banner is required when logging on to any device connected to the Kentucky Information Highway (KIH) or any network within the KIH. This policy supports the principles of the Enterprise Security Architecture as expressed in Enterprise Security Domain 5000.

Applicability: This policy is to be adhered to by all agencies and employees within the Executive Branch of state government.

Responsibility for Compliance: Each agency is responsible for assuring that employees within their organizational authority are aware of the provisions of this policy, that compliance by the employee is required, and that intentional, inappropriate use may result in disciplinary action pursuant to KRS 18A, up to and including dismissal.

It is also each Executive Cabinet's responsibility to enforce and manage this policy. Failure to comply will result in additional shared service charges to the agency for the Office for Technology's efforts to remedy intrusion activities resulting from unauthorized usage where insufficient security notice was not provided by the agency.

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). The EDU CIO is responsible for authorizing all changes to the PPM.

Policy: All logon screens must include a security notice that states the involved system may be used only for authorized purposes.

Specifically, the notice must state the following:

- Only authorized users may access the system.
- Users who access the system beyond the warning page represent that they are authorized to do so.
- Unauthorized system usage or abuse is prohibited and subject to criminal prosecution.

- System usage may be monitored and logged.

Security notices should not contain specific information about the organization, operating system, network configuration, or other internal information, thus making it more difficult for unauthorized users to exploit system vulnerabilities. In addition, the security notice should not include words that imply consent to use the computer system such as “greetings" or "welcome.”

Minimum Required Security Notice

Notice: This is a government computer system and is the property of the Commonwealth of Kentucky. It is for authorized use only regardless of time of day, location or method of access. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy. Any or all uses of this system and all files on the system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized state government and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using this system, the user consents to such at the discretion of the Commonwealth of Kentucky. Unauthorized or improper use of this system may result in administrative disciplinary action and/or civil and criminal penalties. By clicking “OK” you acknowledge your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

OK

Review Cycle:
Annually

Timeline:
Revision Date:
Review Date: November 29, 2011
Effective Date:

Enterprise Security and Policies
Cross Reference # http://technology.ky.gov/governance/Pages/policies.aspx
CIO-79—Logon Security Notice

OTS Standards
Cross Reference #