YOUTH SERVICES
POLICY

Title: Access to and Use of Computers Assigned to Employees **Next Annual Review Date:** 07/10/2010	**Type:** A. Administrative **Sub Type:** 5. Information Services **Number:** A.5.2
	Page 1 **of** 3
References: Act 772 of the 2001 Regular Session of the Legislature, and Division of Administration's Office of Information Technology Standards	
STATUS: Approved	
Approved By: *Mary L. Livers, Deputy Secretary*	**Date of Approval:** 07/10/2009

I. AUTHORITY:

Deputy Secretary of Youth Services (YS) as contained in La. R.S. 36:405. Deviation from this policy must be approved by the Deputy Secretary.

II. PURPOSE:

To establish the Deputy Secretary's policy regarding access to and use of state-provided computers.

III. APPLICABILITY:

All employees of Youth Services. Each Unit Head is responsible for ensuring that all necessary procedures are in place to comply with the provisions of this policy.

IV. DEFINITIONS:

Computer Equipment - Includes computer file servers, desktop/notebook computers, data communications equipment, personal digital assistants (PDA), and Blackberries.

Unauthorized Access - Ability to view, add, modify, delete, print, copy, or transmit data from an information system where the individual gaining access does not have the right or the need to know such information.

Unit Head - Deputy Secretary, Chief of Operations, Assistant Secretary, Undersecretary, Deputy Assistant Secretaries, Deputy Undersecretary, Facility Directors, and Regional Managers.

YS Central Office - Offices of the Deputy Secretary, Chief of Operations, Assistant Secretary, Undersecretary, Deputy Undersecretary, Deputy Assistant Secretaries, and their support staff.

V. POLICY:

It is the Deputy Secretary's policy to make computers available to employees to perform their job duties. Computers must be used for official business only. All other uses are strictly prohibited. Access to an employee's computer by a youth in the custody or under the supervision of YS is strictly prohibited except for instructional use at schools/libraries within the facilities. All employees using computers are responsible for ensuring the security of their assigned computer equipment and preventing unauthorized access and use.

VI. PROCEDURES:

A. Appropriate computer software that is necessary for the employee to perform his job duties shall be installed on an employee's assigned computer. Personal software is strictly prohibited without the authorization of the Information Technology (IT) Director.

B. Software from outside vendors or other governmental agencies may be installed, with approval from IT, on the computers to meet an internal need or to participate in a multi-agency initiative. The use of such software must not compromise YS' computer security infrastructure. Any violation of policies established for the use of such software, resulting in the disclosure of classified information to unauthorized persons, injury or loss to the system, unauthorized modification or destruction of system data, or loss by theft of any computer system media, may result in disciplinary action.

C. All computer software must have a registered license. Software products used throughout YS for email, anti-virus, and the information systems are licensed through IT.

D. Employees are prohibited from changing a computer's hardware or system settings, opening the computer case to remove, replace, or repair components, or having computer administrator rights to their assigned computer unless authorized by the Unit Head.

E. All Windows desktop/notebook computers must be configured for automatic Windows Updates.

F. At a minimum of once every two weeks, all employees assigned use of a notebook or laptop computer are responsible for ensuring that the laptop/notebook computer is turned on and attached (via network cable) for a minimum of one hour to allow anti-virus and operation system updates.

G. At least once a month, or when Microsoft issues a security threat alert, all Windows file servers and computers must be updated with the latest Windows Updates.

H. Information stored on the computers is the property of the State of Louisiana. All information that Unit Heads determine to be critical to their operations must be saved on a regular basis to a removable media (computer tape, CD, external hard drive, etc.) and stored in a secured area or saved to a fixed media, such as dedicated back-up file server.

I. All desktop and notebook computers must be configured to activate the screen saver password protect feature upon a maximum of 30 minutes with no keyboard/mouse activity.

J. All computer equipment must conform to applicable Division of Administration, Office of Information Technology Standards. The Director of IT is responsible for ensuring the dissemination of applicable standards to all units.

K. Employees must report state tag numbers and produce computer equipment when requested by inventory control staff.

L. Employees are not to give their passwords to anyone. Information Technology staff may request an employee's password in order to troubleshoot a problem under the employee's ID. If Information Technology staff request a password, once they are finished, the employee must change their password.

Previous Regulation/Policy Number: A.5.2
Previous Effective Date: 12/19/2008
Attachments/References: