Texas Youth Commission **GAP.05.07**
General Administrative Policy Manual

Chapter: Agency Supports and Controls
Rule: Agency Use of Information Resources

ACA Standard(s): 4-JCF-6F-05

Effective Date: 12/15/08, T-92
Page: 1 of 3
Replaces: GAP.05.07
Dated: 5/31/06, T-78

(a) **Policy.**

The Information Resources Division (IRD) exercises uniform control and standards for the design, development, implementation, security, and maintenance of an organized system of information. IRD regulates agency acquisition and use of all information technology resources. IRD operates under the direction of the Assistant Deputy Executive Director for Information Technology in coordination with agency user groups and executive management.

(b) **Explanation of Terms Used.**

(1) **Information Technology Resources –** The procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information. These include, but are not limited to, information technology systems, hardware, software, information systems, and communication systems.

(2) **Information Technology System –** A group of hardware and software that works as a unit. A typical system would include a desktop computer, monitor, printer, and software.

(3) **Information Technology Hardware –** Equipment designed, built, operated, and maintained to process information. It includes, but is not limited to, desktop computers, notebook computers, monitors, printers, pagers, phones, cell phones, personal digital assistants, and facsimile machines.

(4) **Information Technology Software –** Code or programs that use and control the capabilities of information technology hardware. This includes commercially packaged software, internally developed programs, freeware, and shareware.

(5) **Information System** – A group of interconnected information technology resources providing data and information in various forms. The intranet and internet are examples of information systems.

(6) **Communication System –** Equipment and programs that provide transmission, emission, or reception of signs, signals, writings, images, or sounds of intelligence of any nature by wire, radio, optical, or other electromagnetic systems. This includes, but is not limited to, telephone, radio, pager, and cellular telephone systems.

(c) **Responsibilities.**

(1) The design and implementation of information technology systems will be performed in accordance with IRD's programming and operations standards and the information technology project management process.

(2) IRD assesses agency application and technology needs.

(3) IRD assesses the effectiveness of information technology systems in meeting agency needs and identifying ways to improve and secure information technology resources and services. The effectiveness of the information system as it relates to overall facility management is evaluated in writing annually.[1]

[1] ACA standard 4-JCF-6F-05

(4) IRD incorporates appropriate security in all information systems design.

(5) IRD is responsible for establishing, modifying, disabling and deleting TYC network and e-mail accounts and system accesses.

(6) Disposal of information technology resources shall be in accordance with state accounting property rules and procedures.

(d) **Security.**

(1) Any use of information technology resources for personal business or any business other than that specified in state security rules and procedures according to Texas Administrative Code 1 TAC §§ 202.1-202.8 and authorized by TYC is grounds for disciplinary action up to and including termination of employment.

(2) TYC information systems will contain a notice and consent banner stating the rights of the agency and the responsibilities of those accessing TYC information systems.

(3) Access to agency information systems requires approval from the information or application owner and/or concurrence from IRD.

(4) Employees and other users of agency information systems must maintain exclusive control and use of their user ID(s) and password(s) and are responsible for any activity, authorized or unauthorized, resulting from the use of their user ID(s) and/or password(s).

(5) Employees and other users of agency information resources are required to secure their assigned information technology resources from unauthorized use.

(6) Employees and other users of agency information resources are required to secure their assigned mobile information technology resources to include physical protection.

(7) Supervisors shall notify the Central Office Human Resource Management Department and IRD upon learning of an employee’s decision to terminate or change location or when an employee is placed on administrative leave pending disciplinary action to ensure removal of access to all TYC information technology resources.

(8) Supervisors shall notify the Central Office Human Resource Management Department and IRD immediately when a decision is made to withdraw an employee’s right to access TYC information technology resources.

(9) The local human resources administrator (HRA) shall notify the Central Office Human Resource Management Department and IRD when employees begin an extended leave of absence (greater than 30 days), due to FMLA, recall to military duty, etc.

(10) Non-TYC employees, including but not limited to contractors, employees of contractors assigned to TYC, and volunteers, shall have access to TYC information technology resources approved by the TYC administrative authority. TYC administrative authorities shall reconfirm on a periodic basis that access is still needed and to notify IRD immediately when access is no longer required.

(11) IRD may monitor any TYC information technology resource to ensure security and appropriate use of state property and time without notice of times, locations, or durations.

(e) **Information Technology Software.**

(1) Information technology software may not be installed on any agency information technology resource without prior approval from IRD.

(2) Employees who use any unauthorized information technology software may be subject to disciplinary action up to and including termination of employment.

(3) Information technology software applications and modifications are developed to meet specific agency needs through the information technology project management process in coordination with the information or application owner and in conjunction with IRD.

(f) **Information Technology Hardware.**

(1) IRD must approve all information technology hardware for agency use.

(2) Employees assigned information technology hardware are responsible for ensuring its proper use.

(3) Employees who modify or cause damage to information technology hardware through negligence or misuse are subject to disciplinary action up to and including termination of employment.