GEORGIA DEPARTMENT OF CORRECTIONS Standard Operating Procedures		
Functional Area: Office of Information Technology	**Reference Number:** IVJ01-0001	**Revises Previous Effective Date:** 5/01/00
Subject: Technology Policies & Procedures		
Authority: Wetherington/Ferrero	**Effective Date:** 12/31/01	Page **1** of **10**

I. POLICY

It is the policy of the Georgia Department of Corrections (GDC) that the Office of Information Technology (OIT) will provide and assume the responsibility for the procurement, delivery, maintenance and support for the information technology environment of the agency solely or via State approved processes.

II. APPLICABILITY

All state correctional institutions, transitional centers, probation detention centers, probation diversion centers, boot camps, other facilities and offices operated by the Georgia Department of Corrections. All employees within the Department of Corrections, its contractors or sub divisions, and other part-time employees of the Department.

III. RELATED DIRECTIVES

A. O.C.G.A: 16-9-90

B. GDC-Rules: 125-1-1.09, 125-1-2-.02, 125-1-2.04

C. Standard Operating Procedures: IIA0503, IVJ0201

D. ACA Standards:

IV. DEFINITIONS:

Computing environment Refers to all computers and processors of all types used for data manipulation, transmission, or storage. It includes all hardware, software, connectivity devices, storage devices, printers, modems, cabling, servers, monitors, and keyboards, mouse-pointing devices, speakers and multimedia peripherals that were bought, provided or maintained by OIT. Generally it applies to those computer related devices and software that assist the user in the performance of their business activity. It does not include embedded

computing devices such as perimeter detection monitoring computers, control room fire/safety monitoring units, inmate telephone systems, access point devices, and so forth.

Software Any computer application, purchased off the shelf or developed from code or developed from a purchased shell program. Any application loaded on any computer or server within the Georgia Department of Corrections.

Hardware The physical part of a computer system, the machinery and equipment. Hardware consists of the computer system's CPU (central processing unit), disks, CDs, keyboard, modem, monitor, cables, printer, and so forth.

V. ATTACHMENTS:

N/A

VI. CONTENTS

VII. PROCEDURES:

This document contains the standard operating procedures pertaining to the computing environment in the Georgia Department of Corrections.

VIII. Total Cost of Ownership

The Total Cost of Ownership (TCO) is a financial figure derived from the actual cost of placing a computer into use in the Department of Corrections work environment for authorized users. This figure is an all inclusive one that begins with the purchase of the user workstation but also extends to the software installed on it, its license, service, network access prorating; WAN costs for installation

and monthly recurring fees; use of central office servers, their purchase, applications; central office developers and maintenance engineers, just to mention some of the behind the scenes costs. This is not an all-inclusive list. The TCO can, very generally, be derived by dividing the number of computers in the agency into the overall OIT budget. For example, the TCO for 1999 was $2727 per computer workstation. (Return to Contents)

IX. Purchasing:

The Georgia Technology Authority (GTA) is the only authorizing body in the State of Georgia with the authority to grant permission and approval to purchase computing equipment, regardless of the source of money (GDC budget, grants, etc.). All purchases must be approved via OIT through GTA. Procedures for what must have prior approval versus routine purchases are outlined in GTA procedures and purchasing work flow diagrams. Purchasing in the Georgia Department of Corrections for computing related items (software, hardware, peripherals, etc.) will be handled through the OIT Business Office. Payment for such items may originate from a variety of sources but will comply with this policy in all aspects. This will help ensure that standard items are introduced into our environment and help minimize the maintenance and trouble calls. (Return to Contents)

X. Computing Hardware

A. Assignment:

The placement of computers within the agency will be determined by a combination of the requesting user, proper approval from Division Information Systems Coordinators (DISC) or Directors with sufficient business justification, security, and the technological feasibility of the location (considering connectivity and functionality limitations).

B. Relocation:

Computer equipment is <u>not</u> to be moved from one location to another without the knowledge and approval of OIT. If the computing needs change for any reason, OIT should be contacted to express those needs and request assistance. Requests will be considered and addressed as resources and policy allow.

1. Most workstations are configured with the software and hardware interface devices to comply with the user's needs. Movement of a workstation, or any of the equipment making up that workstation, may cause conflicts, logon failures, incompatibilities, and unnecessary support calls and/or return of the workstation to the original location. Generally, moves can be accomplished with little or no trouble within the same

segment or LAN location; however, it should not be attempted without OIT approval.

2. All GDC staff and sites are accountable for the computing equipment inventory at the location to which it is assigned. Once the equipment is placed at a site, it can be moved from that site only by OIT staff or its authorized maintenance vendor/contractor or via common carrier or courier services authorized by OIT.

C. Equipment Replacement and Upgrade:

OIT has, as part of the Technology Strategic Plan, the vision of maintaining a refreshed level of computing capability. This is to be accomplished by identifying approximately the oldest 25% of existing hardware and replacing it annually with new equipment. This can only be accomplished if the appropriate budget funding is available but should keep the equipment at most only three to four years old. The goal is to reduce the maintenance cost of repairing older equipment and to provide users with a reasonably modern computing tool set.

D. Maintenance:

The responsibility for maintaining computing equipment within the agency will be that of OIT. OIT will have each item of authorized equipment inventoried and will use this authorized equipment inventory list to determine maintenance. If the item is not part of the official OIT inventory, maintenance will not be authorized. Maintenance will be accomplished through factory warranty service, field technician on site visits, or OIT central office repair staff. Maintenance may, in some cases, result in replacement of the item.

E. Equipment not purchased via the authorized method will not be maintained or replaced by OIT and will be in violation of this policy. (Return to Contents)

XI. Inventory

A. Inventory Transfers

1. OIT equipment shall be transferred from a site only by OIT staff or its authorized contractors.
2. All equipment transfers will be documented and tracked in the OIT SCRIBE Computer Inventory application.

B. OIT Staff, Authorized Contractors

1. The OIT authorized staff and/or contractors may swap broken equipment during a service call to a site.
2. OIT staff and/or authorized contractors are required to document the change out of equipment. The OIT staff/contractor will document a transfer out of the piece of equipment being replaced on the transfer inventory page in the OIT SCRIBE Computer Inventory application.
3. The OIT staff/contractor will receive the replacement piece of equipment for the receiving site on the Receive Inventory page in the OIT SCRIBE Computer Inventory application.
4. OIT field staff and/or authorized contractors shall not remove the GDC sticker from any OIT equipment.
5. OIT equipment shipped to the local site via common carrier or courier service authorized by OIT will be deemed to have arrived at the site when the transfer form packed with the equipment is signed by the local site. OIT inventory staff will document the transfer out of equipment in the OIT SCRIBE Computer Inventory application. The receiving site should notify the field tech that transferred equipment has arrived. The field tech will accept the transferred equipment on the Receive Inventory page in the OIT SCRIBE Computer Inventory application for the receiving site.

C. GDC Sticker

1. Only OIT may issue a GDC sticker for OIT equipment.
2. OIT will issue a GDC sticker for the equipment swapped out by the vendor at a site. The sticker will be mailed to the site with the instructions for the LISC (Local Information Services Coordinator) or OA (Operations Analyst) to sticker the specific piece of equipment.

D. OIT Inventory

1. OIT inventory will maintain and update a local inventory tracking program identifying equipment, transfer or receipt, GDC sticker number and serial number.
2. OIT inventory will issue all GDC sticker numbers for new OIT equipment or for vendor exchanged equipment.

E. Surplus

1. The determination that equipment will be surplused will be made by OIT. OIT staff will physically surplus equipment and complete the appropriate surplus and inventory documentation.

(Return to Contents)

XII. Software

Software will be provided for the users in the agency. It may be in the form of applications loaded locally on a computer, on a server on a Local Area Network (LAN), or in centralized servers accessed via a Wide Area Network (WAN).

A. OIT will maintain a master list of software and will publish it on the GDC Intranet (Captiva) under Information Technology. Only that software needed for business and deemed appropriately licensed will be allowed. Licensing records will be maintained via OIT purchases and records.

B. Any use or installation of any software from any source other than that authorized by OIT will be in violation of this policy. Companies that police software usage are hired by major vendors to identify abuses. Federal authority regulates their access to our computers, and they can obtain access upon request.

C. In addition to placing the agency in jeopardy, any person violating this policy may be subject to personal liability for fines.

D. Any person needing software for a legitimate business purpose should request it through their Division Information Systems Coordinator (DISC).

(Return to Contents)

XIII. Computing Environment

A. Appropriate Use:

GDC computing equipment is purchased for authorized individuals for the intended business purposes for which the equipment was purchased. The limited or occasional personal use of equipment and software may be accomplished with the supervisor's permission but

will adhere strictly to the policies outlined in this document governing the use of computers.

B. Inappropriate Use:

The inappropriate use of a computer can be a physical abuse, neglect, or purposeful misuse. It can also be an inappropriate utilization of the equipment or software that would violate usage, security, or access policies and procedures. It can also include negligence in maintaining the data kept within the storage devices or drives. Care should be taken to protect the computing equipment from extremes in temperature, moisture, damage, or any other damaging environmental hazard or exposure. Care should be taken to insure the safety of diskettes, CDs, tapes or any other means of storage of data. (Return to Contents)

XIV. Internet Access

The use of GDC provided Internet access imposes certain responsibilities and obligations on users and is subject to state government policies and local, state, and federal laws. As a condition of being granted Internet access by GDC, each employee must comply with this policy and refrain from inappropriate and/or prohibited use at all times.

Information and files composed, transmitted, or received on GDC equipment may be considered part of the GDC records. Employees should ensure that all information accessed with or stored on GDC equipment is appropriate, ethical, and lawful.

Unnecessary Internet usage causes network and server congestion, slows other users, takes away from work time, and could over burden other shared resources. Because of this, accessing/downloading large audio or video files is strictly limited to business purposes only.

A. Appropriate Use

1. Federal, state, or local government Internet sites.
2. Access to sites related to professional organizations or other professional development information.
3. Downloading of technical bug fixes, patches or drivers used by OIT for providing the latest updates to software and applications.
4. Job-related research.
5. Other supervisor approved usage.

B. Inappropriate Use

1. Any use of the Internet (WWW) that is not in the best interest of the Department of Corrections will be considered inappropriate. Inappropriate Internet use includes, but is not limited to:
   a) Private or personal for-profit activities. This includes business or solicitations related to commercial ventures, religious or political causes, or any matter related to outside organizations.
   b) Knowingly downloading or distributing pirated software, information, or malicious program code (viruses).
   c) Downloading any software or electronic files without ensuring that GDC-provided virus protection is active.
   d) Uploading or downloading commercial or agency software in violation of copyrights or trademarks.
   e) Playing games and “chatting”.
   f) Performing any activity that could cause the loss or corruption of data or the degradation of system/network performance.
   g) Any other activity that would reflect discredit on GDC.

C. Prohibited Use

1. Any use of the Internet (WWW) for the following purposes is strictly prohibited:
   a) Accessing or downloading pornographic or sexually explicit material.
   b) Accessing or downloading material that could be considered discriminatory, offensive, threatening, harassing, or intimidating.

c) Conducting any illegal activities as defined by federal, state, or local laws or regulations.

d) Gambling.

D. Internet Usage Monitoring

1. Employees with access to the Internet should be aware that any information accessed, downloaded, or transmitted may be reviewed by system's staff and agency management. While GDC respects the privacy of its employees, the importance of ensuring appropriate use of state resources may result in the occasional monitoring of Internet sites visited by GDC employees. Inappropriate Internet usage can expose the GDC to significant legal liability and reflect discredit on the department.

2. When using GDC computers and resources to access Internet sites, employees are consenting to the monitoring of their use and have no reasonable expectation of privacy in the use of these resources.

3. OIT staff is required to notify agency management when inappropriate material is discovered on GDC computers or when a review of Internet sites visited indicates misuse.

E. Penalties for Misuse of Internet Access

1. Employees using GDC provided Internet access agree to adhere to the policies and guidelines established by the department. Alleged violations of this policy will be reviewed on a case-by-case basis.

a) Internet access can be revoked at any time.

b) Clear and willful violations or abuse of what is considered to be acceptable use will be subject to appropriate disciplinary action, up to and including termination from employment.

c) In appropriate circumstances, criminal or civil action may be initiated.

F. Purchasing ISP Accounts

1. The purchase of Internet access accounts must be approved by Division Information System Coordinators (DISC) or Directors, and will be reviewed for conformity to standards by the Office of Information Technology. The responsibility of the payments for ISP accounts, modems, modem lines, and any services associated with the access to the Internet will be the responsibility of the section under which the facility or

office falls. The Office of Information Technology is not responsible for these payments. (Return to Contents)

XV. Security

The introduction of information technology throughout the Georgia Department of Corrections (GDC) has resulted in the GDC becoming heavily dependent on the availability of reliable information technology to meet its business needs. The networks that facilitate our ability to instantaneously share information may also allow unauthorized persons to gain detrimental access to information technology resources in the GDC network.

A. Detrimental access to the GDC enterprise network is defined as any intervention, from either an internal or external entity, that creates any situation whereby authentication and access control mechanisms are bypassed that may compromise the confidentiality or integrity of information resources or render it unavailable. OIT Security Administration will proactively track detrimental access activity and work to prohibit or correct such activity.

B. Detrimental access may be intentional or unintentional. Where unintentional detrimental access activity is detected, the affected individual will be advised to correct exploitable vulnerabilities to prevent future occurrences. Where detrimental access activity is determined to be intentional, it will be assumed as malicious activity and an appropriate response will be initiated.

C. The Georgia Computer Systems Protection Act (O.C.G.A. 16-9-90) specified unlawful acts involving information resources and the subsequent penalties upon conviction. As data residing or transiting State networks and equipment is held in public trust, it must be afforded the greatest safeguards. Therefore, computer security policies, procedures, instructions, processes, and standards created in furtherance of protecting GDC computer assets rely upon the Georgia Computer System Protection Act (O.C.G.A. 16-9-90) to ensure compliance. Violators may be prosecuted accordingly.

The Georgia Department of Corrections security policy, procedures, and processes are outlined in SOP IVJ0201. Please refer to that document for security procedures. (Return to Contents)