

DARTON

COLLEGE



Information Technology Security Policy

March 2008

INFORMATION TECHNOLOGY SECURITY POLICY

TABLE OF CONTENTS

Statement of Direction

- Principles
 - Specialized Technical Staff
 - Users of Electronic Assets
- Internet

Risk Assessment

Darton College Information Technology Security Policy

- Purpose
- Principles
- Scope
- Enterprise Roles
 - Department of Campus Information Services
- Roles and Responsibilities
 - Department Head
 - Chief Information Officer
 - Security Associates
 - Specialized Technical Staff
 - Application Development Staff
 - Production Support Staff
 - LAN Administration Staff
 - Information Custodians
 - Users of Electronic Assets
 - Passwords
- Access to Published College Information
 - Access to College Information Under the Open Records Law
 - Exemptions to the Open Records Law
 - Routine Internal Use and Maintenance of College Information
- Physical Access
 - General Introduction and Requirements
 - Workstation Security
 - Darton Faculty and Staff Workstations
 - Faculty and Staff Lab Workstations
 - Student Lab Workstations
 - Classroom Workstations
 - Specialized and Shared Work Areas

- Passwords and Combinations
 - Backups
 - Archives and Records Management
 - Laptop and other portable technology
 - Dial-up access
 - Home Placement of State-Owned Computer Equipment
- Risk Assessment
- Computer Crime
- Escalation
- Training
- Monitoring

STATEMENT OF DIRECTION

The goal of the College is to establish and maintain a proactive security policy. All users of the College's electronic data processing assets will know how to access a copy of the security policy and be familiar with its contents.

PRINCIPLES

- Assignment of Responsibilities: The College will create and maintain a document that clearly identifies the individuals who provide security for each platform for the College.
- Consistency of Security Provisions: The College will have consistent access controls across platforms. While the objective may be technically impossible at this time due to lack of adequate software, every effort will be made to be aware of new products on the market and their potential to accomplish this objective.

The College will develop a policy for resetting passwords. This policy will include: identification of individuals authorized to reset passwords, identification of who may request resets, procedures to be followed in making a request, and a strategy to authenticate the person making the request.

- Separation of Duties: Limited Staff size and a large number of applications spread across all platforms make total separation of duties a difficult task. However, the separation of duties between access to rules and access to data will continue to be high-priority objective. Project managers and supervisors will include this principle when assigning duties to Applications Development Staff, Production Support Staff and LAN Administrators. Supervisors and management will incorporate this principle when filling vacancies or defining division and department structure.
- Audit ability: The College will establish standards for creation and maintenance of security rules, logon ids and user ids. Standards will include documentation of specific types of access granted to each role, i.e. Security Associates, Help Desk Staff, etc. Procedures will also be defined for requesting changes, documentation required, and retention of that documentation.

Logging of potential risks as well as violations will be performed on all platforms.

Review of all log reports and monitoring will be included in annual performance standards. Well-defined procedures for investigation of potential problems will be disseminated to all personnel whose duties include monitoring.

All requests for logon ids, user ids, or access must be signed or logged by the Security Associate.

Specialized Technical Staff: Roles and Responsibilities

Applications Development Staff

The Office of Information Technology (OIT) will establish distinct test, pre-production, and production libraries. Procedures for transfer of programs, scripts, and other types of library members will be documented. When available and advisable, based on risk assessment, software will be utilized for version control and to provide backups.

Personnel who are familiar with the College programming standards, the Applications Development and/or Production Support staff, and the platform should complete transfers between libraries. Transfers should not be assigned to an individual who only knows a checklist of steps to complete and does not have knowledge of transfer implications. OIT may consider the use of the security associates to perform library transfers.

Users of Electronic Assets: Roles and Responsibilities

OIT will develop a standard written Information Technology Security Policy and Information Confidentiality Notification that all users, regardless of platform, must sign. Access requests will include commitment statements to ensure confidentiality and a warning of possible monitoring. Users must also acknowledge the necessity to prevent abuse and misuse of the workstation. The intended user of the logon id or user id and his/her supervisor must sign the request. To expedite access for new employees, a logon id or user id and necessary security may be granted, but no passwords should be provided until the forms are signed. Each user will be given a copy of the signed form.

OIT will devise one or more processes to annually remind users of their security policy responsibilities. A timetable will be determined for users to sign a new acknowledgement of confidentiality.

RISK ASSESSMENT

Risk Assessment will continue to be a process of balancing the need for confidentiality, data integrity, and availability, with perceived customer service. Risk Assessment will be a major consideration for all aspects of the College Information Technology Security Policy. It should be completed during the analysis and design of applications and prior to the procurement and installation of equipment and software.

Care should be taken not to evaluate risk based solely on current requirements. For example, an application may only be needed by one or two people in a central location when it is designed, but in time a program could grow to an extent that the application is requested by a large number of people, including those in remote locations.

Risk Assessment should include representatives from the user community, the Chief Information Officer, Security Associates, and the Inventory Supervisor for items over \$100,000.

DARTON COLLEGE INFORMATION TECHNOLOGY SECURITY POLICY

PURPOSE

The purpose of this document is to define and clarify the policies, principles, guidelines, and responsibilities related to the security of the College's information technology resources.

PRINCIPLES

The College acknowledges the standards and expectations established by the University System Information Technology Security Guidelines. The College's principles reflect the Policy and provide further direction:

- Assignment of Responsibilities: The College has a Statement of Direction regarding the roles and responsibilities related to securing information resources.
- Consistency of Security Provisions: The College has controlled and known access controls across platforms (e.g., mainframe, network, Internet) used to retain, access, or transport the information. The Statement of Direction contains additional goals.
- Separation of Duties: The College has a Statement of Direction that is designed to administer security responsibilities separate from other duties that might result in compromises to the protection of the College's information resources.
- Expectation of Appropriate Security: Users of the College's information processing facilities can be confident that the facilities are secure and provide reasonable protection to the information the College retains or transports.
- Audit Ability: The College has a Statement of Direction to establish clear, straightforward standards to document who has access to change the security rules, when changes were made to the security rules, and to report attempted violations of the security rules on all platforms.

SCOPE

This policy applies to all Darton College employees. The Office of Information Technology has statutory responsibilities that are described in the section on Enterprise Roles. When statutes are available, their requirements will take precedence over these policies.

The policy applies to the College's students, contractors, business partners, and others authorized to use the College's information technology resources.

Implementation of this policy helps to insure that the following characteristics apply to information technology resources of the Department:

- *Confidentiality* - sensitive information is protected against unauthorized access.

- *Integrity* - information is protected from tampering, unauthorized modification, or falsification.
- *Availability* - legitimate users of the College's information technology resources can access those resources in a timely manner.

ENTERPRISE ROLES

Office of Information Technology (OIT)

On behalf of the enterprise, OIT will:

- Maintain security administration tools adequate for departments to control access to the information held, processed, or transported by the department on their behalf. Provide training and procedures for the use of these tools.
- Administer security for OIT staff and services.
- Assist departments with the implementation of access control decisions.
- Assure that security policy and technology are addressed in enterprise information technology planning and implementation projects.
- Establish college-wide standards for computing and network equipment and configurations that allow for departments to maintain control over access to information for which they are responsible.
- Establish and implement strategies to periodically monitor compliance with security policy standards.
- Identify and publish the name of the custodian of college databases that are established or under development by one or more departments. The custodian will be held responsible for proper distribution of individual access to private college data within the application.
- Ensure new college-wide software tools used to retain, access, or transport data are properly secured.
- Convene the Security Committee (made up of the security administration professionals employed by the college) periodically to gather input on the configuration of the security administration facilities maintained by the College (see 'Security Committee,' below).

ROLES AND RESPONSIBILITIES

The College has identified roles, responsibilities and relationships related to the security of information technology resources of the college.

The roles and responsibilities for security in the College include the following:

Budget Unit Head:

The Budget Unit Head is responsible for the information collected by the unit and for controlling access to that information. The Head of the Unit may delegate specific security responsibilities, but he/she is ultimately responsible for the security of the

college's information and technology assets. The Budget Unit Head has delegated responsibility for custody of the college's records.

Chief Information Officer (CIO):

The College's Chief Information Officer (CIO) is the Director of the Office of Information Technology. The CIO is responsible for the configuration of the College's information technology resources and for the development, promulgation, and enforcement of the agency's security policies.

The CIO is responsible for issuing Statements of Direction that will guide the development and maintenance of security policies, procedures, and relationships among the various information technology security functions within the College. The CIO appoints the Security Associates; all security functions report to the Security Associates who report to the CIO.

College Security Associates:

The Security Associates are appointed by the CIO and are located in the Office of Information Technology.

The Security Associates will:

- Have the appropriate classification to manage security for the College.
- Establish access controls.
- Ensure documentation of information custodians, including personnel authorized to approve production library transfers.
- Identify recommendations for training requirements, frequency of training, provide or assist in arranging for training for the Departmental Security Personnel.
- Develop and implement strategies to make users aware of security policies, procedures, and benefits; determine the frequency of awareness training and information.
- Solicit evaluation of the effectiveness of training provided and/or arranged.
- Document the security support structure across platforms.
- Communicate the direction for College security standards, procedures and guidelines.
- Enforce college security policies.
- Notify other departments when staff who have access to data in those departments leave or have significantly changed duties.
- Be aware and maintain a copy of the Darton College policies for disposal of equipment.
- Monitor unusual activities, e.g., violation reports.
- Conduct an annual security review.
- Maintain lists of information custodians and security personnel in formats available to all department personnel.

- Work with auditors as directed by the Chief Information Officer.
- Work with the College Physical Security Officer as needed.

The Security Associates are responsible for establishing processes to assure security, and communication with end users, including for example:

- Publishing guidelines to create passwords,
- Standardizing the format and process for all employees to acknowledge an understanding of the security requirements,
- Strategies and processes for regular reminders of the security responsibility of all users.

OIT will require pre-employment screening for individuals who are delegated security functions.

Specialized Technical Staff:

Staff who are directly responsible for security, system management, and applications development have special privileges in relation to information resources such as the ability to examine the files of other users. The number of people with access management rights must be strictly controlled and limited. Access to information technology resources must be restricted on a legitimate need-to-know basis.

Application Development Staff have limited access to production applications. The process for routine review for code changes includes the following:

- There is software available to set controls on changes and to produce reports when changes are made.
- Senior staff can approve and sign off on changes. Junior staff and consultants must request approval and sign off from senior staff, as determined by supervisory or project leader personnel.

Production Support Staff will include Applications Development staff and LAN Administrators, who are granted access to production systems in order to address emergencies that would otherwise result in system unavailability. OIT will maintain a log system to identify and document the emergency and identify which individual fixed the problem. Production Support Staff are to assume that all data has value and may be sensitive; it must be treated as confidential unless there are more specific requirements from the program areas.

Computer Operators and some end-users are granted access to some files, as required to provide service to other state entities and submit department jobs for normal production operation. Computer Operations Staff are to assume that all data has value and may be sensitive; it must be treated as confidential unless there are more specific requirements from the program areas.

Help Desk Staff may have authority to reset passwords.

LAN Administration Staff, based on the requirements of their job, have broad access to systems including access to information on workstation "C" drives. LAN Administrators are to assume that all data has value and may be sensitive; it must be treated as confidential unless there are more specific requirements from the program areas. LAN Administrators can function as Associate Security Officers. LAN Administrators or E-mail Administrators may be specifically authorized to use network management tools that circumvent the normal delivery of messages by intercepting or monitoring the contents of messages addressed to another recipient. The monitoring of messages, use of the Internet, and other forms of network communication must be requested by a supervisor and must be for a specific purpose. When it is an option (e.g. with remote take-over tools) the LAN or E-mail Administrator must advise users in each instance that their messages are being intercepted when the tools are in use. When direct notification is not an option (e.g. with network monitors) the LAN or E-mail Administrator must advise users that their messages may be intercepted in the course of routine network monitoring. The Statement of Direction includes the objective to advise users of the results of monitoring, including potential disciplinary actions. If a supervisor has requested monitoring, only the results of that request are subject to disciplinary follow-up. For example, if a supervisor has requested a search for use of illegal software, disciplinary action should not be initiated for personal use of the Internet.

The security function is controlled and will be documented for all platforms, e.g., mainframe, network, and Internet. The Statement of Direction includes an object to centralize the security function across platforms. Darton College has a computer committee to resolve issues arising from different strategies and technologies used for different platforms.

The Chief Information Officer will assign access privileges based on several factors:

- Matching the privilege to an appropriate job function;
- Balancing the need and timeliness for the privilege against the efficiency of granting access to the data; and
- Taking into account the exposure associated with the privilege with regard to the length of time the access will be needed.

Specialized Technical Staff with broad access to data are in sensitive positions will be required to undergo a security check as a condition of employment.

Information Custodians:

All information custodians are reminded that, based on legal precedents, an individual may delegate authority but never responsibility.

Department Administrators may delegate custody to department employees. Darton College applications development and production support staff may also be given

authority to grant access to department information. However Darton College OIT staff should never be the sole delegate, nor should Darton College OIT staff grant access without written or verbal approval from the department delegate. In all cases, the name(s) of the individual(s) to whom these responsibilities are delegated must be clearly posted and/or published so that all users of the information know who is the legal custodian.

Information Custodians have the responsibility to share security requirements with Application Developers and the College Security Associates or to delegate for confidentiality or specialized treatment of data that stem from federal, statutory, or other requirements. Information Custodians will establish the standard for record retention for their data and will authorize the disposal of records.

Information Custodians must notify the Chief Information Officer when an employee leaves or there is a significant change in duties that affect the need for access to information resources. The Chief Information Officer will distribute the information to the appropriate Security Associates.

Information Custodians, Application Development Staff, and Darton supervisors working with contractors who are authorized to access the college's information resources must notify the Chief Information Officer when a contractor leaves or there is a significant change in duties or schedule that impacts the need for access. The Chief Information Officer will disburse the information to the appropriate Security Associates when applicable.

Users of Electronic Assets:

Users of Electronic Assets of the College include any employee of the College, student, business partner, contractor, consultant, or customer who is authorized to use the information technology assets of the College.

OIT requires a written request form, which includes a security acknowledgement and signature of the user, for mainframe access. The Statement of Direction will establish a process to include a similar procedure for other platforms. The Statement of Direction will also establish a process to annually remind users of their security policy responsibilities. The process for authorizing user logon should be the same regardless of the technology accessed, i.e., mainframe, network, or Internet.

The Chief Information Officer will develop and disseminate guidelines and examples for users to assist them in maintaining good security practices. This material may include brochures, electronic reminders, desk references, web sites, etc. and should include but not be limited to information on passwords and password protection, logon id, virus protection strategies, etc.

Due in part to licensing requirements and software compatibility issues, Darton College has a policy stating that installation of all workstation hardware and software must be authorized by the Computer Services Workstation Support Group and/or the Network

Support Group. Software includes, but is not limited to, screensavers, computer games, and material downloaded from the Internet.

Confidential information should not be on the workstation hard drive for security and business reasons. Most workstations pose a risk of unauthorized access because the "C" drives are not private or restricted to the user who is normally assigned to a workstation.

Software that includes a terminal locking feature, e.g. screen saver with password protection, must be available to all users. The advantages of this type of software and the techniques for its use are included in the training of new personnel. The use of password protection and terminal locking is mandatory for the CIO and security associates.

An example for users on Password Protection guidelines include:

Passwords must be:

- Confidential
- Between 5 and 8 alphanumeric characters long
- With the exception of temporary passwords created by the Security Associate, the owner of the user id must create passwords.

Good choices for passwords are:

- Two or more adjoining words
- Gibberish
- Alphabetic characters mixed with numbers

Poor choices for passwords are:

- Repeating character strings
- A single dictionary word
- Trivial. Never use:
 - Any part of your name
 - Nicknames
 - Initials
 - Spouse's or child's name
 - Your user id
 - Hobbies
 - Seasons of the year
 - Birthdays
 - Anniversary dates
 - License plate numbers
- Passwords, including those assigned by Security Associates, should never be **PASSWORD** or the user's login id or user id.

- Passwords should be difficult to guess, but easy to remember so that you do not need to write them down. Passwords that are written down should never be left in easily accessible locations, e.g. unlocked desk drawers, desk calendars, the back of the workstation.
- When changing a password don't use one you have used recently.
- The UNIX systems will require you to change your password(s) at least every 180 days. Staff in positions of high-risk, e.g. security associates, LAN administrators, must change their password(s) at least every 90 days.

User ids are disabled after three failed attempts on the mainframe and after 5 failed attempts on other platforms.

Network management tools that circumvent the normal delivery of messages by intercepting or monitoring the contents of messages addressed to another recipient are used only by employees specifically authorized to use such tools. When it is an option (e.g. with remote take-over tools) users are advised that their messages are being intercepted when the tools are in use. When direct notification is not an option (e.g. with network monitors) users are advised that their messages may be intercepted in the course of routine network monitoring. Notification must be made for each occurrence where tools give the option to view confidential data or change data in any way.

The contact for questions or additional information is the Chief Information Officer.

Access to Published College Information

A "record" is broadly defined to mean ". . . any material on which written, drawn, printed, spoken, visual or electromagnetic information is recorded or preserved, regardless of physical form or characteristics, which has been created or is being kept by an authority. "Record" includes, but is not limited to, handwritten, typed or printed pages, maps, charts, photographs, films, recordings, tapes (including computer tapes), computer printouts and optical disks.

The college routinely publishes information which is of general interest to the public and which does not carry confidentiality requirements. The mechanisms for publication range from traditional pamphlets and books to documents accessible through the world wide web. Access to published documents is not limited to specific individuals and the security provisions necessary for published documents generally only include those necessary to assure integrity and availability.

Examples of published college information include the College employees' telephone and email directory and the Athletics Calendars.

Access to College Information under the Open Records Law

The Open Records Law: Georgia's Open Records Law is "to be construed in every instance with a presumption of complete public access, consistent with the conduct of

governmental business." All requests for information under the Open Records Law should be forwarded to the Vice President for Business and Finance for approval and processing before any records are released.

Exemptions to the Open Records Law:

The Open Records Law contains three types of exemptions:

- Exemptions expressly set forth in the Open Records Law.
- Exemptions based on exemptions to the Open Meetings Law.
- Common law exemptions.

Exempt records:

1. Specifically exempted from disclosure by state or federal law.
2. Investigative information obtained for law enforcement purposes.
3. Record is a computer program.
4. Trade secret.
5. Record would identify a law enforcement informant.

Examples of exempt records include:

- Drafts, notes, preliminary computations and like materials prepared for the originator's personal use.
- Materials which are the personal property of the custodian.
- Materials to which access is limited by copyright, patent, or bequest.
- Published materials in the possession of an authority, other than a public library, which are available for sale or available for inspection at a public library.

In addition, the Open Records Law states that its inspection and copying rights do not apply to a record which has been or will be promptly published with copies offered for sale or distribution.

The Open Records Law gives public access to existing records. Staff should not do additional programming to make the data more meaningful, unless so directed by management. An example of this is a record that contains a code, which relates to a title stored in another file or table; the code may not be self-explanatory, but Darton College staff should not, as a matter of course, write a new program to create a unique file including the title within the record.

Routine Internal Use and Maintenance of College Information

Internal use of information is limited to specific individuals performing specific work tasks:

Most use and maintenance of information retained by the college is conducted outside of the provisions of the Open Records Law. Routine access to information is generally conducted by employees or other agents of the college. Approval for such routine access is not granted under an Open Records request but is done when specific work assignments are made which require the access.

OIT has designated people who will issue logon ids and user ids. Specifically, these people are located in OIT. The logon id/user id will:

- Provide access only to the extent needed to perform the work for which the access is granted.
- Provide access only of the type (create, read, update, delete) needed to perform the work for which the access is granted.
- Provide access only for the time period during which the work is performed.

Identification of individuals using college information (other than individuals using low security applications such as informational web pages and the college employee telephone directory):

OIT will issue separate user identification (user id) to each person who is authorized to access information retained by the college. Each person will also be issued a temporary password that is to be changed at the first logon and maintained according to a regular schedule. Persons issued a user id and password are responsible to others. Persons issued a user id are responsible for all information accesses performed under that user id.

PHYSICAL ACCESS

General Introduction and Requirements

The College has established controls over physical access to critical or sensitive hardware and the physical environment of that hardware for Darton College. In addition to following the Darton College guidelines, OIT has established more stringent controls over access to the mainframe and enterprise network environment. Physical access to network servers or multi-user systems may result in access to data on those systems. Physical controls also minimize the threat of theft and downtime caused by accidental or deliberate disruption.

All computer platform administrators at Darton College must work in cooperation with the College's staff in OIT, Inventory Control, and with the Chief Information Officer to implement physical access and environmental control measures to protect the College's computing infrastructure. These security measures, which cover routers, gateways, bridges, all types of servers, desktop and laptop computers, and other mobile technology, should be commensurate with the value placed on the assets by the Department. Security measures should not adversely affect productivity and should be appropriate for the facility where the equipment is located.

All reasonable efforts should be made to ensure the safety and security of the hardware that comprises the Darton College Network. There are two categories of technology equipment:

- Equipment that has data stored on it has more stringent security requirements;
- Equipment that does not have data stored on it must be subject to prudent procedures and practice.

The following measures should be taken to physically safeguard the Department's information technology equipment and environment.

1. Risk Assessment & Security Review

The Department Head, or other department-assigned person, for each Department must periodically assess the physical security of information technology at each network site. The Departments' plans for security must be submitted to the Chief Information Officer for approval. The Chief Information Officer, the Security Associates, the Inventory Control Supervisor, and the Vice President for Business and Finance will periodically review security procedures in all Departments.

2. Access Control

All Department production file, database, and communications servers and all other critical network related equipment should be in secure environments; test files and equipment should be secured when possible, but less emphasis is put on these. In all situations, the list of individuals who have access to secured areas must be on file with the Chief Information Officer and Security Associates.

Various techniques can be employed for access control:

- Persons in secure rooms wear visible personal identification or visitor badges;
- Access doors can be electronically secured and alarmed 24 hours a day with access only by individualized magnetic cards;
- Combination locks may be used. Where these locks are utilized, the combination will be made available to staff under the same policies as other access, including audibility. A designated staff person will change the combination whenever there are staffing changes and on a prescribed schedule at other times. The combination will follow manufacturer's suggestions, e.g. multiple numbers simultaneously. Only the designated staff may share the combination with other personnel.
- Attempts to defeat physical security controls can be prohibited;
- Permanent right to access can be granted and removed by Division/Department Security Associates strictly on a regular need-to-be-there basis;
- Visitors can be escorted by staff with permanent access.

3. Physical Environment

The measures taken to assure a secure physical environment should be appropriate to the equipment to be protected. Measures that will be taken unless the physical location precludes implementation include:

- Rooms should have adequate fire and water detection, prevention, and suppression controls and emergency lighting;
- Water sprinklers should not spray on the equipment;
- Temperatures within the room should be maintained within operational limits;
- Telephones should be within easy reach of all equipment;
- Smoking, eating, or drinking will be prohibited in the vicinity of critical equipment, e.g., servers; prudent care should be taken when in the vicinity of non-critical equipment;
- Combustible materials, such as paper, should generally be stored outside of the area. If it is necessary to store special forms in a physically secured area, personnel in the secured area will be aware of the potential problems.
- Windows should be permanently locked, non-existent, or inaccessible from the outside;
- The equipment should not be viewable from outside the building; and
- Critical equipment such as servers should be physically secured to a large and/or immovable object, but not in such a way as to restrict technical maintenance.

4. Disposal of Equipment

Information technology equipment will be disposed of in accordance with policies established by the State of Georgia.

Workstation Security

Reasonable efforts should be made to safeguard individual workstations. Workstations can be secured by securing the rooms where they are located and by physically attaching them to tables or work areas so that special tools are required to remove them from the premises. Darton College also requires the following: .

- Passwords should not be built into the logon script for auto-signon.

Darton College Faculty/Staff Workstations

Faculty and staff are on site during normal business hours from 8:00 a.m. to 5:00 p.m. Due to flexible schedules and project requirements, faculty/staff may be on site both earlier and later. While this does not prevent public or unauthorized access to software and hardware used by the faculty/staff, it may provide a deterrent.

Student Workstations

Student workstations are available in the main computer lab during the posted hours. A student lab assistant should be on duty for all hours of service. Students should be monitored by a college employee when using computers in labs or classrooms. Computer classrooms are locked when classes are not in session.

Specialized and Shared Work Areas

The Darton College multi-media lab, which is also used for storage of some hardware and software, is open during regular business hours but is locked at night and on weekends. (However, maintenance and cleaning staff have a key to the door.)

The Darton College Computer Operations Room is kept closed and locked and requires a special key to open. Unauthorized personnel, including applications developers, are to be accompanied by permanent, authorized personnel when it is necessary to enter the Computer Operations room. Maintenance and cleaning staff only have access when accompanied by authorized personnel.

The College workstation set-up room is kept locked. Only Workstation Support team members are authorized to access the area.

Mainframe computer hardware and software are secured and controlled by policies maintained by the Campus Information Services Department.

Servers for production applications for systems used by staff located in the Administration building must be located in the Computer Operations room. Servers for production applications for systems used in other buildings are kept as secure as possible. Building design may preclude the use of a locked area.

Passwords

Passwords for the production servers are modified at least every 90 days. More frequent changes are required when staffing changes occur.

Backups

All mainframe programs and files are backed up routinely. Please refer to the Institutional Security Plan and Report. The Applications Development team will coordinate requirements with the Disaster Recovery procedures established by OIT. Backup procedures for an application will be written and provided to the CIO.

An incremental backup of each server is done daily, and a full backup is done once each week. All backup tapes are retained for six weeks and are stored offsite. The Applications Development team, the Chief Information Officer or a representative, one or more members of the Network Support team, and the department personnel responsible for the

data will develop disaster recovery procedures for the application. The procedures will be provided to the Chief Information Officer.

Archives and Record Management

The CIO will establish policies and procedures in accordance with statutory requirements and data-specific requirements established by the Information Custodian. If desired, the Chief Information Officer may delegate this task to the Security Associates, but final approval and responsibility will remain with the Chief Information Officer.

Laptop and other portable technology.

Portable technology refers to any model designed to be carried from place to place, such as notebook, laptop, cell phones, LCD panels, etc. This equipment may be connected to a mainframe for terminal emulation where modems and authority are provided.

The following applies to all uses of portable technology:

- Darton College employees or consultants who are granted this permission may check out portable equipment. Availability is on a first come, first served basis.
- The work unit responsible for the unit will maintain a checkout log. This log, which may be electronic, should include the user's name, date of pick-up and return, and where the equipment will be used. Check-out and check-in procedures will also include an inspection of the equipment, e.g. requisite cables and spare parts.
- All users of portable equipment will receive notice on how to safeguard the equipment, including safeguards against temperature damage.
- Portable equipment and related software may only be used for Darton College business.
- All copyright laws must be observed. Use of state property for personal gain, or by non-Darton College employees, except for authorized consultants, is prohibited.
- Where appropriate to the equipment and the location, it must be plugged into a surge protection device and kept in a locked, protective carrying case when not in use. Where possible, the equipment should be placed in a locked file or supply cabinet.
- Portable equipment should not be checked as luggage on airlines and should be under observation at all times.
- Equipment should not be left unattended unless appropriately secured.
- Equipment should not be left in a vehicle where it could be exposed to temperature damage or theft.
- Be observant of surroundings when using equipment on the road to access college systems.

Dial-up Access

In some cases, job duties require dial-up access to the mainframe and/or network. Requests for dial-up access will require justification, access request procedures similar to those for a user id and logon id, and written approval by the Chief Information Officer. A list of individuals with dial-up access will be maintained by the Security Associates and will be available to those assigned to monitor any access activity.

Home Placement of State-Owned Computer Equipment

In some cases, job duties require mainframe and/or network access from home and it may be undesirable to check out a Department laptop or use an individual's personal computer. Requests for a state-owned computer to be placed in one's home will require justification, signoff by the employee's supervisor, and written approval from the Vice President for Business and Finance, and finally, a computer must be available for long-term loan. A copy of the written approval should be sent to the Chief Information Officer and the Inventory Supervisor. The Chief Information Officer will maintain a list of individuals with home computers, and this list will be available to those assigned to monitor any access activity.

RISK ASSESSMENT

Security is a critical application design feature. Darton College will continue to use technology to secure data, e.g., security components of the Windows 2000 platform for the network. Risk must be assessed in relation to the following factors:

- Quality of the control mechanism
- Size of the threat
- Potential loss

Strategies for Security are cumulative and include:

- Low security required. Routine data backup, mechanisms to detect data corruption, and refresh corrupted data. Group ids are appropriate at this level only for general purpose/general access. The response to a security threat at this level is follow-up to determine the source of the threat depending upon the consequences of that threat to the agency.
- Medium security required. Equipment is kept in locked facilities, user authentication is required at the time of access, individual user ids are required, passwords are encrypted, list of user ids to verify passwords, tools to assure that the individual accessing the system continues to be the person who logged on, possible time-out during long sessions to verify that the legitimate user continues to be the person accessing the system. The response to a security threat results in an examination of the source(s) of the threat.

- High security required. Equipment is kept in access-controlled facilities. Security measures include logging of users and access times, intruder detection alarms, regular security audits, encryption, and individual user ids. Network access of this device(s) should be excluded from access through the firewall. The response to a security threat results in energetic efforts to investigate the source of the threat and to implement strategies to prevent the threat from reoccurring.

Examples of Risk Assessment:

1. Failure to protect information that is confidential -- High Risk and High Quality Security Needs may result in severe consequences from unauthorized access. One example is a student record where the data owner may suffer fines and/or job loss if there is unauthorized access due to inadequate protection.
2. Failure to protect access to the information where there is Low risk and Low Quality Security Needs may result in few or minimal consequences. Low risk/low security may be deliberate in order to encourage or authorize access. Examples in this category include a web page or the college employees' telephone directory.

While risk assessment is something of a subjective evaluation, the following questions will be considered prior to the acquisition of new hardware and software, as well as new applications development. In many cases the questions should be asked of business and program staff, not just OIT personnel.

The following questions may be useful to business/program area managers to consider in determining the need for security for proposed applications, especially in relation to Internet applications:

1. Who are the intended users of this application?
 - General Public (are your users a subset of the general public, e.g., Georgia residents only, businesses only, individuals)
 - Partners (current/potential contractors, clients, those regulated, other)
 - Staff of one Department to staff of another Department
 - Employees
 - Students
2. What is the potential consequence of unauthorized access to the information?

For example if there are serious consequences such as fines or firing that result from the access, then there is a need for High/rigorous security. If the consequences include a reprimand, minor political or some minimal financial embarrassment, then there is a need for Medium security strategies. If there are

minor consequences or the application is one where you actually want to encourage access, then the need for security is Low.

Consider the following as you define your need for security:

- To what degree do you need to protect the information from unauthorized users? (Access Control) __H __M __L
- To what degree do you need to prevent confidential information from exposure to the public? (Confidentiality) __H __M __L
- To what degree do you need to protect the data from alteration, forgery, or accidental tampering? (Data Integrity) __H __M __L
- To what degree do you need to confirm that the data/request is coming from the individual or source you think it is coming from? (Authentication) __H __M __L
- To what degree do you need to confirm that the information you are sending/receiving can only be received or sent from the person intended? (Non-repudiation) __H __M __L
- Is it necessary to prove the accuracy and integrity of the record at some point in the future, e.g., date, parties involved? __ N __ Y
- Does the proposed application require a signature (by law or current practice)? __ N __ Y

COMPUTER CRIME

All users of information technology resources who are issued a user id must receive a copy of the state statute on Computer Crimes.

Some examples of policy violations include:

- Accessing or attempting to access another individual's data or information without proper authorization (e.g., using another person's password to look at their personal information)
- Obtaining, possessing, using, or attempting to use someone else's password regardless of how the password was obtained
- Tapping phone or network lines (network sniffers)
- Making more copies of licensed software than allowed
- Sending an overwhelming number of files across the network (e.g., spamming or e-mail bombing)
- Intentionally releasing a virus or other program that damages, harms, or disrupts a system or network
- Intentionally preventing others from accessing services
- Unauthorized use of state resources
- Sending forged messages under someone else's id
- Using state resources for unauthorized or illegal purposes
- Unauthorized access to data or files even if they are not securely protected.

ESCALATION

If an exposure to a breach of security is identified, report the exposure to the Chief Information Officer as soon as possible. The CIO will determine:

- The best course of action.
- The number of individuals who need to know about the exposure.
- If the exposure is beyond the Department's boundaries and will affect the College. If so, the CIO will report the exposure to the Vice President for Business and Finance, Vice President for Academic Affairs or Vice President for Students Affairs as appropriate.

TRAINING

The College's CIO will arrange for training for the Security Associates and those to whom the CIO has delegated authority. This training will address responsibility, authority, requirements for access and exemptions to access.

The College's CIO will regularly participate in training regarding responsibilities to design, implement, maintain, and upgrade a sound configuration of the College's information technology assets. The CIO will also participate in training regarding strategies to train security staff in security responsibilities.

The College's Technical Specialists, e.g., LAN Administrators, Production Support Staff, and Application Developers will participate in training regarding their unique roles and responsibilities in relationship to system development, ongoing operations, and confidentiality. Information Custodians in the Departments will participate in training regarding their respective roles as custodians of agency data.

All department users of electronic assets of the college will receive training regarding college security policies and procedures and their respective responsibilities in relation to protection of the college's information technology assets.

MONITORING

Compliance with security policies will be monitored using the following strategies:

- Network management tools that circumvent the normal delivery of messages by intercepting or monitoring the contents of messages addressed to another recipient are used only by employees specifically authorized to use such tools.
- The Georgia Department of Audits and Board of Regents' Auditors conduct system level review of security practices related to financial information within agencies and develops recommendations for improvement.