DARTON COLLEGE

Institutional Security Plan and Report

December 31, 2007

2400 Gillionville Road
Albany, GA 31707
(229) 317-6704
(226) 430-2926 FAX

Institutional Security Plan & Report
December 2007

I. Institution Profile

Institution Name:	Darton College
Date Submitted:	December 31, 2007
Individual Responsible for the Report:	Margaret Bragg, Director, OIT/CIO

TYPE & SIZE
Darton College is a two-year college in the University System of Georgia. The college provides network/Internet access to its faculty and staff via workstations connected to the campus network. Students are provided network/Internet access via workstations located in six student computer labs and in the college's library.

The college consists of eleven main buildings, each having access to the campus network. The college has servers that provide access to faculty, staff, and students to major IT services such as PeopleSoft, BANNER, Xtender, Axiom, Luminis for student email, Exchange for faculty and staff mail, Blackbaud for Development, Blackboard ID card system and the college web site. To assist in protecting these servers and the campus workstations attached to the campus network, the college has installed a Cisco firewall. In addition, the college utilizes a Cisco Intrusion Prevention System.

RISKS

1. ***Unauthorized / malicious network access from "outside" campus network*:** The magnitude of this risk should be greatly reduced by the CISCO firewall. In addition, the college utilizes a CISCO Intrusion Prevention System (IPS). The IPS also monitors all "inside" campus network traffic for malicious activities. //Details later in the Plan//

2. ***Climate control systems in critical server room*:** The room that houses the college's critical systems has a primary and a backup temperature control system to ensure that the temperature in the room remains at a level suitable for the critical servers to operate safely. In addition, the Climate Control Systems are connected to the server room generator.

3. ***Installation of unauthorized software on computers located in student computer labs***: To ensure that unauthorized software cannot be utilized on the computers located in the classrooms, student computer labs, library and public computers, the college utilizes Deep Freeze security software on computers in which the Deep Freeze Software has been installed, the application automatically removes unauthorized software that has been installed on the computer; thus assisting the computer services department in maintaining functional consistency on all student computer lab and library workstations. Checks are made nightly to see if there are updates to Virus Date or Microsoft. If updates exist the computer is thawed, then updated, installed, and the machine is shut down for the night.

4. **Some common types of computer security risks are:**

   Acts of god: Such as tornados, earthquakes, fire, lightning, floods, etc., can carry a high price. A well designed and tested contingency recovery program can reduce the recovery

time and efforts, as well as reduce the final cost.

Sabotage by employees: Damage done by an employee with access to the system can be extensive, since there may be few warning bells once a person has gotten into an actual program. Deliberate sabotage by outsiders: This could include vandalism, manipulation of data or programs, destruction of data, programs or hardware.

Loss of confidentiality: The loss of confidentiality due to an unauthorized person's access to sensitive information. This could take the form of a person looking at confidential personnel records or classified government information.

Viruses: The damage done by viruses could include destruction of software or hardware, destruction or alteration of data, or simply the tying up of resources for a period of time resulting in costs to the institution.

Theft of hardware: Theft of hardware includes the theft of any computer or computer-related equipment, including connection lines. Access security is important to prevent this type of security risk.

Unauthorized use of hardware or software resources: Any unauthorized use of hardware of software, whether it be for personal or business reasons.

Carelessness: Running the wrong program, hitting the wrong key, putting in incorrect information, running a program out of order, and other acts of carelessness can have a very small to catastrophic impact on data and software programs.

Computer crime: This might include embezzlement, disclosing secret information, selling of data, fraud, willful destruction of data, unauthorized use of state resources, etc.

Damage from environmental conditions: Damage can occur from failure to control temperature or humidity, particulate and chemical contaminants, magnetic field radiation, smoking, etc. the computing area.

ORGANIZATION & STAFFING

The Office of Information Technology is responsible for all aspects of design, installation, service, and support for the following areas of computing: hardware, software, dissemination of electronic data, communications, user support, helpdesk services, application and development support, network services, telecommunications, strategic development, and research implementation of new technologies. This service encompasses both academic and administrative computing on both campus locations and support of additional institutional presence at other locations. The Office of Information Technology is comprised of three functional areas to accomplish this support: Client Support Services, Network Support Services, and Enterprise Application Services. In addition, to the support of faculty, staff , and students, several major systems are also supported: Banner Student Information System (Student, Financial Aid, General, Accounts Receivable, Georgia Mods), Banner Web (Student, General, Faculty Advisor), Banner Xtender with Axiom, Peoplesoft Financials (Budgets, Accounts Payable, Accounts Receivable, Purchasing), Peoplesoft HRMS (HR, Payroll), Compass Testing, Aceware-Continuing Education, Blackboard-DataCard Services, Pharos Student Printing, RDMS-Document Imaging, Inventory, Web Services, effollet-Bookstore, and Exchange Groupware (Email, Calendaring, Document Sharing). Furthermore, all telecommunications for the college are the responsibility of the Chief Information Officer and IT Department as well. This includes all voice and data circuits, user support, and

communications with ITC DeltaCom, the PRI provider.

II. Institution-wide Policies and Security Procedures

a. Institutional Acceptable Use Policy

The Information Systems Use Policies is a campus-wide policy intended to cover acceptable use of all Darton College computing and network resources. The Information Systems Use Policies are located on the Darton College Web site at http://www.darton.edu/oit/index.php and is included in this document. Electronic Mail Security and Managing Passwords Policies are included in the Information Systems Use Policies document.

b. Personal Security

Training Users
All Darton College technical personnel will complete the WebCT Security Course for administrators. All other personnel will complete the End User Security Course by the end of Spring Semester. New employees will be required to complete the course as a part of the employment process. A mechanism for training students using the WebCT class will be developed for students by Fall Semester 2006.

Darton College Information Technology Security Policy

Reporting and Handling Security Incident Response Policy

III. Protection of Critical Institutional Computing Resources

Classifying Assets (4-1) (Enterprise Level Legally Protected Repositories)
Critical Server Assets

Handling Information (9-1) (Secure Handling, Storage)
Data Stewardship and Access Policy
Information Systems Ethics Policy
Sensitive Information Protection Policy
Wireless Access Policy

Disposing of Media (9-2)
Disposal of Media Policy

Securing Physical Entry to Restricted Areas (6-2)
Darton College Information Technology Security Policy

Securing Power Supplies (6-5)
Darton College Information Technology Security Policy
Minimum Information Security Environment Policy

Controlling Access to Networks and Systems (12-5)
Darton College Information Technology Security Policy

Data Stewardship and Access Policy
Email System Acceptable Use and Security Policy
Internet Services (Server) Registration Policy
Minimum Information Security Environment Policy
Network Connections for Surveillance System Cameras and Digital Recorders Policy
Remote Access Policy
Sensitive Information Protection Policy
Wireless Access Policy

Protecting Against Malicious Software (8-6)
Anti-Virus Software Policy
Information Systems Ethics Policy
Minimum Information Security Environment Policy

Implementing Encryption Techniques (13-4)
Remote Access Policy
Sensitive Information Protection Policy

Developing Back-up Procedures (10-1)
Critical Systems Back-up Policy

DARTON COLLEGE

Information Systems Use Policies

December 1, 2007

2400 Gillionville Road
Albany, GA 31707
(229) 317-6704
(226) 430-2926 FAX

College Information Systems Use Policies

1.0 Introduction

Darton College's Information Systems are critical resources and play an integral part in the fulfillment of the College's objectives of teaching, research, and extension of knowledge to the public. The **Darton College Information Systems Use Policies** provide guidelines for the access, use and protection of these resources.

College Information and information resources shall be used in an approved, ethical, and lawful manner to avoid loss or damage to College operations, image, or financial interests to comply with official policies and procedures. Students and personnel shall contact the Chief Information Officer prior to engaging in any activities not explicitly covered by these policies.

2.0 Purpose

The purpose of this document is to summarize and provide in a single location all approved policies aimed at ensuring that the access, use and protection of the Information Systems promotes the College's objectives. These Policies will achieve the following principles:

- ensure that Users abide by state and federal laws, as well as the policies of the College and the University System of Georgia;
- ensure that all individuals accessing or using the Information Systems assume responsibility for protecting these resources from unauthorized access, modification, destruction or disclosure;
- ensure the integrity, reliability, and availability of the Information Systems; and
- ensure that individuals do not abuse the College's Information Systems and do respect the rights of members of the College community.

3.0 Scope

This document and the catalogued Policies apply to students, and all College employees, including, but not limited to, faculty and staff. The Policies also apply to all individuals, whether authorized or not, who use the College's Information Systems from any location. Use of the College's Information Systems, even when carried out on a privately owned computer that is not managed or maintained by the College, is governed by these Policies.

The College or University System owns all College information resources; use of such resources constitutes consent for the College to monitor, inspect, audit, collect and remove any information without permission or further notice. Students and personnel shall be trained in what use is acceptable and what is prohibited. The college regards any violation of this policy as a serious offense. Violators of this policy are subject to college disciplinary actions. Offenders may be prosecuted under the Georgia Computer Systems Protection Act (O.C.G.A. 16-9-20) and other applicable state and federal laws.

4.0 Designation of Representative

4.1 College President shall be responsible for the following:

The President of Darton College shall be responsible for ensuring appropriate and auditable security controls are in place.

4.2 Vice Presidents and Executive Council Members shall be responsible for the following:

- Informing personnel of College policies on acceptable use of information resources.
- Ensuring that personnel under their supervision comply with these policies and procedures.
- Ensuring that non-college contract personnel under their supervision comply with these policies and procedures.

4.3 Vice President for Student Affairs shall be responsible for the following:

- Informing current and new students of College policies on acceptable use of information resources.
- Ensuring that students comply with College policies and procedures.

4.4 System Administrators and Data Custodians shall be responsible for the following:

- Monitoring systems for integrity.
- Maintaining and ensuring data backups of critical electronic information.
- Promptly reporting suspicion or occurrence of any unauthorized activity to the Chief Information Officer or his/her designees.

4.5 All students and personnel shall be responsible for the following:

- Abiding by official College policies on acceptable use of information resources.
- Promptly reporting suspicion or occurrence of any unauthorized activities to the Chief Information Officer or one of his/her designees.
- Any use made of their accounts, logon IDs, passwords, PINs, and tokens.

4.6 The Chief Information Officer (CIO) or one of his/her designees shall be responsible for the following:

- Ensuring the availability, integrity, and confidentiality of the College's information resources
- Addressing violations of College policies on information resources.
- Interpreting College policies on information resources.
- Developing and maintaining the College's information resource security policies.
- Developing and disseminating awareness and training materials.
- Assuring compliance through compliance auditing.
- Reporting compliance findings.

5.0 Terms

User refers to any person, whether authorized or not, who makes any use of any Information Systems from any location.

Information Systems includes, but is not limited to, computers, terminals, servers, printers, networks, data, modem banks, online and off-line storage media, access card systems, computer integrated telephony, other technology hardware, databases, data repositories, metadirectories, and related equipment.

6.0 Compliance

Violations of these Policies may result in the discipline of an individual in accordance with applicable College policies or state or federal law, including criminal prosecution. The College may temporarily suspend, block, or restrict access to Information Systems when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of Information Systems or to protect the College from liability.

7.0 Reporting Violations

Users shall report alleged violations of any of the catalogued Policies to the College's Chief Information Officer who will investigate the alleged violation and, if appropriate, refer the matter to College disciplinary and/or law enforcement authorities. Alleged violations of Policies will be pursued in accordance with the appropriate disciplinary procedures for faculty, staff and students, as outlined in the Faculty Handbook, Employee Handbook, the student Code of Conduct, and other applicable materials.

In addition, Users shall report security incidents such as unauthorized use of their accounts, harassment, abuse (including abusive or offending e-mail communications), or unauthorized access to their computer files and directories.

8.0 Appeals

Users found in violation of any of the catalogued Policies may appeal any imposed disciplinary action in accordance with the appeals provisions of the relevant disciplinary procedures.

9.0 Administrative Procedures

This document, and any of the catalogued Policies, may be changed by the Information and Instructional Technology Committee, with such changes being reviewed and recommended through

the Executive Council. The Office of Information Technology (OIT) will prepare, coordinate, and process all recommended changes.

10.0 Policies

The following chart catalogs the current **Information System Use Policies** in practice at Darton College.

Policy	What is it?	Who does it apply to?	What needs to be done?
Anti-Virus Software Policy	Requires mandatory use of Anti-virus protection for Windows and Macintosh computers	Anyone at Darton with a personal computer connected to the College network	Install a copy of Anti-Virus on all computers connected to the College network
Data Stewardship and Access Policy	Defines “College Information” and how it will be controlled and accessed.	Anyone at Darton who accesses College information	Access to College information requires approval by the appropriate Data Steward; see the Procedures section for specifics
Disaster Recovery and Data Backup Policy	Requires backup of critical system ensures effective resumption of vital functions in the event of unscheduled interruptions.	Anyone at Darton with a personal computer _____ Anyone at Darton who maintains a server	Backup of users data _____ Backup of all critical servers
Disposal of Media Policy	Requires proper disposal of electronic media containing sensitive data.	Anyone at Darton storing identity or personal information about other people on electronic media	Users are responsible for taking appropriate steps to ensure that all computers and electronic media are properly sanitized before disposal.
Email System Acceptable Use and Security Policy	Describes how College email systems will be managed and protected	Anyone at Darton who uses email _____ Anyone at Darton who maintains an email server	Use strong passwords; do not send confidential information via email; follow procedures to send email messages to large numbers of Darton recipients _____ Indicate on-going compliance to the email server security standards in this policy
Information Systems Ethics Policy	Requires appropriate and civil use of network resources; describes institutional protection of user information	Anyone at Darton using the College’s computing and networking resources	Read the “Appropriate Use” and “College Access to User’s Information (Privacy)” sections.
Internet Services (Server) Registration Policy	Registration of all devices connected to the College network that serves information to on- or off-campus users.	Anyone at Darton installing a server	Register the server and apply security patches; see the Procedures section for details

Minimum Information Security Environment Policy	Minimum precautions for securing computing devices and access to the Darton network. Responsibilities of the Information Security Officer.	Anyone at Darton using computers or having responsibility for a server	Don't use computers or systems you are not authorized to use; don't send an email as if you were someone else; use the College-supported versions of Windows, Mac OS, and Linux; Exchange, VPN (Virtual Private Network) and Anti-virus clients; follow the password generation rules for creating passwords; don't share userids and passwords; maintain documentation to verify proper licensing of purchased software; physically protect your computer or server; do not attempt to defeat the security of information systems.
Network Connection of Surveillance System Cameras and Digital Video Recorders Policy	Approval and configuration requirements for video systems used to protect resources or personnel.	Anyone at Darton planning to install a digital surveillance system	Contact the Chief Information Officer prior to acquisition and installation.
Remote Access Policy	Off-campus access to network and systems are through approved methods only.	Anyone at Darton providing access to local servers from off-campus locations _____ Anyone accessing a Darton network or information system from off-campus	Read the policy and follow the outlined standards and procedures. _____ Use a Virtual Private Network (VPN) client for authentication and encryption; see Procedure for details.
Reporting and Handling Security Incident Response Policy	Steps for reporting and handling security incidents.	Anyone at Darton using computers or have responsibility for security.	How to report an incident. How to manage incidents. Collection and sharing of information guidelines.
Sensitive Information Protection Policy	Protection of systems holding Social Security Numbers, credit card numbers, and other identity or personal information.	Anyone at Darton storing identity or personal information about other people on desktops or servers	If you store bulk social security numbers, credit card numbers, HIPAA (Health Insurance Portability and Accountability Act – medical information), student data (grades, test scores, etc.), bank account numbers on a server you are responsible for or on your personal workstation, read this policy or contact the Chief Information Officer.

Student Computer Access Policy	Requirement for students to have access to computers for Darton College course work.	Student at Darton	All students must have access to a computer; it is the responsibility of students to ensure their access to computers. At a minimum, the computer must provide access to the worldwide web using a current browser, spreadsheet capability and word processing.
Wireless Access Policy	WiFi/802.11 access through centrally managed authenticated methods.	Anyone using a wireless device at Darton	Read the Procedures sections on “Configuration, Installation, and Management” and “Unauthorized Access Points”

Anti-Virus Software Policy

POLICY:

Passive anti-virus detection and removal applications will be installed and activated on all Windows or Macintosh desktops, workstations and laptops/notebooks which are either physically or remotely connected to the Darton College network. Individual users are responsible for ensuring their personal desktops, workstations, and laptops/notebooks are protected by a personally-owned, licensed copy of anti-virus detection and removal application before the device is connected either physically or remotely to the College network.

Rationale:

The rising frequency of security incidents involving network-attached devices significantly increases the probability of major disruptions to the internal computer systems of the College. Statistics indicate that a very large percentage of potentially damaging incidents can be avoided by the use of existing anti-virus detection and elimination procedures. Establishing policy centrally and issuing standards and utilities from a central authority allows for rapid incident response and continuous update of protection methods.

Standards & Procedures:

Standards:

Compliance. Chairs and Vice Presidents are responsible for monitoring compliance by their respective users with this policy and associated standards by: (1) directing users of Windows or Macintosh computers in their respective departments that are provided by the College and connected to the College network to notify the Office of Information Technology (OIT) when an attempted or suspected virus infection has occurred; and (2) directing reviews of, and action on, reports on compliance with this policy that are generated by the Office of Information Technology (OIT). Individual users are responsible for ensuring compliance with this policy and its associated standards for personal machines connected to the College network.

Anti-Virus Software. The College provides a site-wide license for McAfee VirusScan for use on all college-owned machines. Installation will be performed by OIT personnel and will be configured for automatic scanning and automatic updates. Users who know of or expect interference between the anti-virus software and another application running on their desktops, workstations, or laptops/notebooks must contact the OIT Help Desk for evaluation and, if applicable, implementation of work-arounds.

Procedures:

Data Stewardship and Access Policy

POLICY:

All College information will be used with appropriate and relevant levels of access and with sufficient assurance of its integrity in compliance with existing College policies, laws, rules, and regulations.

Rationale:

Reasonable procedures need to be provided for the College community to follow to ensure that valuable College data can be utilized appropriately with guidelines for management and access to data. Roles and responsibilities need to be defined and applied to those in stewardship positions regardless of the actual purpose of the information system.

Standards & Procedures:

Standards:

This policy applies to College Information only (as defined below) and is intended to improve access to these data by employees for conducting College business. In all cases, applicable statutes, rules, and regulations that guarantee either protection or accessibility of institutional records will take precedence over this policy. While this policy is especially pertinent to information stored electronically, it is applicable to all information, such as paper, microform, and video, as well as the content of confidential meetings and conversations. This policy does not apply to notes and records that are the personal property of individuals in the College community and is not directed to data whose primary purpose is scholarly (e.g., instructional material, research notes)

College Information. A data element is considered College Information if it provides support to and meets the needs of units of the College.

Guidelines for determining College Information. Must meet one or more of the following:

a) It is used for planning, providing, managing, reporting, or auditing a major administrative function
b) It is included in an official College administrative report
c) It is used to derive an element that meets the criteria above

By default, all College Information will be designated as INTERNAL DATA for use within the College or to satisfy College external reporting requirements to the Board of Regents of the University System of Georgia, State, Federal, or other external agencies. College employees will have access to these data for use in the conduct of College business. These data, while available within the College, are not designated as open to the general public unless otherwise required by law.

Data Categories. Data stewards are responsible for categorizing all College Information data elements within their managed systems into one of three categories: Confidential, Sensitive, or Unrestricted.

Confidential data. Requires the highest levels of restriction due to risk of harm that may result from disclosure or inappropriate use. This includes information whose improper use or disclosure could adversely affect the ability of the College to accomplish its mission, records about individuals requesting protection under the Family Educational Rights and Privacy Act of 1974 (FERPA), or data not releasable under the Georgia Open Records Act or the Georgia Open Meetings Act.

Sensitive Data. Users must obtain specific authorization to access these elements since unauthorized disclosure, alteration, or destruction will cause perceivable damage to the College. It is assumed that all administrative output from the central administrative systems is classified as sensitive unless otherwise indicated. The specification of data as sensitive should include reference to the legal or externally imposed constraint that requires this restriction, the categories of users typically given access to the data, and under what conditions or limitations access is typically given.

Unrestricted Data. No access restrictions. Available to the general public.

Data Access and Stewardship Procedures. Data users are expected to access College Information only in their conduct of College business, to respect the confidentiality and privacy of individuals whose records they access, to observe any ethical restrictions that apply to data to which they have access, and to abide by applicable laws, rules, regulations, or policies. Data stewards will work together to define a single set of procedures for requesting access to sensitive elements of College Information and to document these data access request procedures. Data stewards also have the responsibility for documenting the meta-data about their data so that users are aware of the definitions, restrictions, or interpretations, and other issues which ensure the correct use of the data.

Functional Data Classifications. Data stewards represent functional areas of the College as defined by the primary purpose served by the data. A functional unit may be given authority for data that is shared by many organizational units of the College.

Auxiliary Data. Supports the auxiliary and related enterprises of the College such as retail sales, central supplies, and other services.

Development/Alumni Data. Supports all aspects of alumni and development data. This includes personal data, demographic data, income, and giving data.

External Relations Data. Supports activities, which interface between the College and the rest of the community. This includes Event Ticket Sales, publications and public information.

Facilities Data. Supports the facilities and services resource of the College including space planning data, construction, maintenance and operational data, reservations and physical descriptive data.

Financial Data. Supports the management of fiscal resources of the College and includes accounting, budgeting, purchasing, accounts payable, accounts receivable, loans, investments, capital assets, inventory, and payroll information.

Human Resources Data. Supports the management of employee resources of the College. This data includes employee demographics, benefits, retirement and EEO data, vitas, employee evaluations, promotion and disciplinary data.

Information Technology Data. Supports the provisioning and management of the technology infrastructure provided by Information Systems and Technology. This includes email addresses, registry and directory data elements not belonging to another data type, network data, and systems data.

Library and Information Resource Data. Supports the management activities and information resource collection activities of the College libraries, including databases of purchased and locally produced information and digitized files of College archives and other special collections.

Person Registry Data. Supports the management of identity and authentication for individuals associated with the College, including the creation of unique data elements (such as DCid, MyDC user name, Library Barcode) that provide unambiguous identification and resolution for merging of identity records. Person Registry data can be used to provision other applications that are managing privileges to authorized individuals or groups.

Student Data. Supports all phases of a student's relationship with the College from application through alumni status except as noted elsewhere. This includes, but is not restricted to, demographic data, academic record, disciplinary and medical records, course information, admissions data, and financial aid, as well as employment with the College, which is dependent on student status.

Procedures:
Request for Access to College Data

Office of the Registrar
Darton College
Request for Access to Restricted Data

1. REQUEST FOR ACCESS [to be completed by Requesting Supervisor]

A. Need for Access

1. Identify the employee for whom access to the Student Records and Schedule of Classes files is being requested.

(Full) Name:_____

Employee ID/SSN:_____ (Former Name)_____

Title:_____

Department:_____

User ID:_____

2. Is this person replacing an employee who had access?

If yes, who _____and did this person leave this position for another at Darton? (Y N)

Should access to the Student Records system be deleted for this person? (Y N) If yes, ڤ Immediately ڤ Future date _____

3. The general duties of this person include (check all that pertain):

ڤAdvise students on their academic progress/requirements
ڤEvaluate applications for admission
ڤMaintain student records/monitor academic progress
ڤCoordinate course offerings and class scheduling
ڤLook up student information
ڤOnly public (directory) information
ڤPublic and restricted information
ڤCoordinate student class roster and grade collection
ڤDevelop and submit programs to retrieve student or course information. If so, what student and course populations will be reported?

ڤHas employee had BANNER training? ڤYes ڤNo

B Access to Data

Check the boxes of the data categories below that pertain to the kind of access this person needs. Note how the information will be used, for example, advise students, monitor academic progress, etc. The use of information must relate to the responsibilities of the person as noted on page 1. Also, note in the Use of Information column any specific online screens to which the requestor needs access. Unless noted, access will be evaluated based upon general responsibility profiles.

Category of Data	Access Type On-line Screen Retrieval		Use of information and Specific Access if applicable
	View	Update	
Student Academic	☐	☐	
Student Address Information	☐	☐	
Student Administrative Data	☐	☐	
Student Course Data	☐	☐	
Student Registration Data	☐	☐	
Student Statistical Data	☐	☐	
Admission Information	☐	☐	
Financial Aid	☐	☐	
Recruiting	☐	☐	
Historical	☐	☐	
Class Roster Data	☐	☐	
Schedule of Classes Data	☐	☐	
Degree Audit	☐	☐	
Degree Information	☐	☐	
Other: _____	☐	☐	
_____	☐	☐	

II. Authorization of Access

ف It is expected that your online access will be added to the Darton College security accounts tables as of _____. Your authorization to access will be included with your BANNER password.

فYour on-line access profile will be released to your Supervisor. It is the responsibility of your Supervisor to orient you to the transactions to which you have been given access. Training for direct access to files will be provided by Darton Office of Information Technology (OIT).

فYour on-line access profile will be released to your Supervisor after an orientation session with the Office of the Registrar contact person. This orientation program will include both general information and specific items tailored to your particular unit's needs, including a description of the current batch and on-line Student Record and Schedule of Classes Systems, the processing schedules for certain types of data, viewing on-line transactions and security.

ف Authorization to the information center files will be issued to you by Darton OIT. Training for access to the files will be provided by Darton OIT.

_____ _____

Signature of Darton College Registrar Date of approval

ACCEPTANCE OF RESPONSIBILITY
(This form must not be completed unless the request for access has been approved by the registrar)

I understand my acceptance of access to the Student Records and Schedule of classes system signifies I accept the responsibility for complying with the institutional policy for the Release of Student Information. I have been given copies of and have read the Release of Student Information policy and the Explanation of Access guidelines. By my signature below, I understand and agree to preserve the security and confidentially of information I access.

I will also inform my Supervisor (who will inform the office of the Registrar) when my need to access student and course data differs from the stated in this Access Request document.

I understand I am responsible for the personal security of my password.

_____ _____

Signature of Darton Employee Date

I am responsible for providing an orientation program for the employee or making arrangements for staff from the office of the Registrar to provide the orientation. I will inform the Office of the Registrar contact person of any changes in status of this employee. I will initiate access deletion if this employee leaves the current position for which he/she has been given approval, and will initiate a new Access Request document for this employee's replacement, if appropriate.

_____ _____

Signature of Supervisor Date

Disaster Recovery and Data Backup Policy

POLICY:

Backup procedures, ensuring that both data and software are regularly and securely backed-up, are essential to protect against the loss of data and software and to facilitate a rapid recovery from any IT failure This document outlines guidelines for Darton College staff on backing up of College Data.

Rationale:

The data backup element of this policy applies to all Faculty, Staff, students and third parties who use IT devices connected to the Darton College network or who process or store information owned by Darton College.

All users are responsible for arranging adequate data backup procedures for the data held on IT systems assigned to them.

The disaster recovery procedures in this policy apply to all Network Managers, System Administrators, and Application Administrators who are responsible for systems or for a collection of data held either remotely on a server or on the hard disk of a computer. The Office of Information Technology (OIT) is responsible for the backup of data held in central College databases.

Standards & Procedures:

Best Practice Backup Procedures. All backups must conform to the following best practice procedures:

- All data, operating systems and utility files must be adequately and systematically backed up (Ensure this includes all patches, fixes and updates)
- Records of what is backed up and to where must be maintained
- Records of software licensing should be backed up
- At least three generations of backup data must be retained at any one time
- The backup media must be precisely labeled and accurate records must be maintained of backups done and to which backup set they belong.
- Copies of the back-up media, together with the back-up record, should be stored safely in a remote location, at a sufficient distance away to escape any damage from a disaster at the main site
- Regular tests of restoring data/software from the backup copies should be undertaken to ensure that they can be relied upon for use in an emergency

Responsibility for Data backup. Only critical systems are routinely backed up by the Office of Information Technology and the other relevant IT managers and systems administrators. The responsibility for backing up data held on the workstations of individuals regardless of whether they are owned privately of by the College falls entirely on the User.

If you are responsible for a collection of data held either remotely on a server or on the hard disk of a computer, you should consult your departmental system administrator or OIT about local backup procedures. If you do not use the facilities provided by OIT or those of your department you should put in place your own procedures.

Legal Requirements. Users when formulating a backup strategy should take the following legal implications into consideration:

- Where data held is personal data within the meaning of the Data Protection Act, there is a legal requirement to ensure that such backups are adequate for the purpose of protecting that data
- Depending on legal or other requirements, e.g. Financial Regulations, it may be necessary to retain essential business data for a number of years and for some archive copies to be permanently retained
- Depending on legal or other requirements, e.g. Data Protection Act, Software Licensing, it may be necessary to destroy all backup copies of data after a certain period or at the end of a contract.

Desktop Backups. The responsibility for backing up data held on the workstations of individuals regardless of whether they are owned privately or by the College falls entirely to the User.

All network users using personal workstations/laptops should ensure that their data is backed up using one or a combination of the following methods:

- Backing-up to a local device e.g. floppy disk, Zip Drive, CD-ROM, USB storage.
- Copying critical data on a regular basis to a server that is properly backed up by the College.
- Backups should be scheduled regularly.
- All users should backup their data before updating or upgrading software on their computers.

Best Practice Disaster Recovery Procedures. A disaster recovery plan can be defined as the on-going process of planning developing and implementing disaster recovery management procedures and processes to ensure the efficient and effective resumption of vital College functions in the event of an unscheduled interruption.

All disaster recovery plans must contain the following key elements:

- Critical Application Assessment
- Backup Procedures
- Recovery Procedures
- Implementation Procedures
- Test Procedures
- Plan Maintenance

Network Managers, System Administrators, Application Administrators. Network Managers, System Administrators, and Application Administrators who are responsible for systems or for a collection of data held either remotely on a server or on the hard disk of a computer must ensure that they have comprehensive, documented and tested disaster backup procedures in line with the best practice guideline in this policy document.

Users. In the case of the loss of a system and data users need to contact the OIT Helpdesk to request replacement hardware. The data will be reloaded from the backup media. Users may also need to re-license software.

Disposal of Media Policy

POLICY:

Increasing amounts of electronic data are being transmitted and stored on computer systems and electronic media by virtually every person conducting business for Darton College. Some of that data contains sensitive information, including student records, personnel records, financial data, and protected health information. If the information on those systems is not properly removed before the equipment is disposed of, that information could be accessed and viewed by unauthorized individuals. As such, all users of computer systems within Darton College, including contractors and vendors with access to Darton College systems, are responsible for taking the appropriate steps, as outlined below to ensure that all computers and electronic media are properly sanitized before disposal. Electronic Media is defined as any electronic storage device that is used to record information, including, but not limited to hard disks, magnetic tapes, compact disks, videotapes, audiotapes, and removable storage devices such as floppy disks and zip disks.

Rationale:

The purpose of this policy is to establish a standard for the proper disposal of electronic media containing sensitive data. The disposal procedures used will depend upon the type and intended disposition of the media. Electronic media may be scheduled for reuse, repair, replacement, or removal from service for a variety of reasons and disposed of in various ways as described below. Printed reports will be shreded before disposal.

Standards & Procedures:

Standards:

What is electronic media? Electronic Media is defined as any storage that is used to record information, including, but not limited to hard disks, magnetic tapes, compact disks, video tapes, audio tapes, and removable storage such as floppy and zip disks.

What is the minimum standard for disposal? All Darton College electronic media should undergo a complete format before the media, or the system containing the media, is surplused or transferred to another department or state agency. If a complete overwrite of the media is not an option, then the media should be destroyed so that the information it is not recoverable without unreasonable time or cost. This standard is necessary to protect all College information, and to comply with software license agreements.

What is confidential information? Confidential Information is important and sensitive material. This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. Some examples of confidential information are system passwords or encryption keys, financial records, proprietary information, human resource or personnel records, student records, and patient records. All media that contains confidential information should be overwritten a minimum of three times with software designed to "zero out" media tracks or destroyed. Other confidential information may be defined by federal or state laws such as FERPA and HIPAA. Examples of solutions for overwriting media are included below.

What are my other options for disposal? Disposal companies can be utilized to remove any media that you wish to have destroyed; some of these companies are listed below.

What should I avoid? Removing the partition information from the media, such as using FDisk, is not sufficient. Reinstalling the operating system, without first completing a full media overwrite is not sufficient. Removing the media and disposing of it in any way that does not render it difficult to recover is not sufficient. Using a magnetic degaussing tool is not reliable for every form of media, e.g. modern hard disks may not be completely erased with most degaussing tools.

Disposal companies:
- Iron Mountain
- Shred It

Software programs that can be used to overwrite media include:
- WipeDrive Pro
- File Shredder
- Eraser
- KillDisk

If you have any questions concerning this standard, or if you would like to suggest a tool that can be added to the list please write to helpdesk@darton.edu

Procedures:

All electronic media must be properly sanitized before it is transferred from the custody of its current owner. The proper sanitization method depends on the type of media and the intended disposition of the media.

Overwriting Hard Drives for Sanitization: Overwriting is an approved method for sanitization of hard disk storage media. Overwriting of data means replacing previously stored data on a drive or disk with a random pattern of meaningless information. This effectively renders the data unrecoverable, but the process must be correctly understood and carefully implemented. Overwriting consists of recording data onto magnetic media by writing a pattern of fluxes or pole changes that represent binary ones (1) and zeros (0). These patterns can then be read back and interpreted as individual bits, 8 of which are used to represent a byte or character. If the data is properly overwritten with a pattern (e.g., "11111111" followed by "00000000") the magnetic fluxes will be physically changed and the drives read/write heads will only detect the new pattern and the previous data will be effectively erased. To purge the hard drive requires overwriting with a pattern, and then its complement, and finally with another pattern (e.g., overwrite first with "00110101 ", followed by "11001010", then "10010111"). Sanitization is not complete until the third overwrite passes and a verification pass are completed. A variety of software packages are available on the open market that properly perform this function.

Destruction of electronic media: Destruction is the process of physically damaging a medium so that it is not usable by any device that may normally be used to read electronic information on the medium, such as a computer, tape reader, audio or video player.

Disposal of Hard Drives: Prior to disposal, operable hard drives must be overwritten in accordance with the procedures above. Equipment designated for surplus or other disposal should have a label affixed stating that the hard drive has been properly sanitized.

Transfer of hard drives within a department: Before a hard drive is transferred from the custody of its current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. All electronic media should be sanitized per standards, however; since the drive is remaining within the department, the hard drive may

instead be formatted prior to transfer. Special recovery tools must be used by an individual to access the data erased by this method; any attempt by an individual to access unauthorized data would be viewed as a conscious violation of state or federal regulations and the Darton College Policies.

Sending a hard drive out for repair or for data recovery: The vendor repairing or recovering data on the hard drive must sign an appropriate agreement with Darton, insuring that the vendor will take proper care of the data. Once data is recovered or the hard drive is repaired, the original hard drive must be returned to the owner so that the owner can dispose of it per this Darton College policy for proper disposal of hard drives.

Disposal of damaged or inoperable hard drives: The owner must first attempt to overwrite the hard drive in accordance with the procedures above. If the hard drive can not be overwritten, the hard drive must be disassembled and mechanically damaged so that it is not usable by a computer.

Disposal of electronic media other than hard drives:

Transfer of electronic media other than hard drives within a department: Before electronic media is transferred from the custody of the current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. Electronic media such as floppy disks, rewritable CD-ROMS, zip disks, videotapes, and audiotapes should be erased if the media type allows it or destroyed if erasure is not possible.

Disposal of electronic media outside of Darton College: All electronic media other than computer hard drives must be erased, degaussed, or rendered unusable before leaving Darton.

Violation of Policy:

If there is a reasonable basis to believe that the proper procedures as outlined in this policy have not been or are not being followed, a report must be filed with the Chief Information Officer. If improperly sanitized electronic media is found, then the media should be reported to the Office of Information Technology.

Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, including but not limited to, termination under the appropriate College disciplinary policy.

Email System
Acceptable Use and Security Policy

POLICY:

Electronic messaging (Email) is an essential and enabling application that facilitates the flow of information within the College and with external correspondents. Electronic messaging systems will be managed and protected across the College in accordance with common standards and procedures.

Rationale:

The College depends on the availability and responsiveness of Email for the normal conduct of College business. The widespread acceptance of Email both within the College and as a part of our personal lives as a means of rapid communication and dissemination of information has lead to the availability of a wide variety of consumer and enterprise applications and services. These applications and systems can be purchased and installed often without regard for the necessary ongoing administrative support needed to maintain system integrity and the security or confidentiality of the information conveyed by the system. For the conduct of College business using email, efficiency of operation and maintenance of security can best be achieved by limiting the number of Email systems serving the College and by using only enterprise class systems to supply email accounts.

Indiscriminate mass emailing to the College community can quickly tax the capabilities of the processing systems to deliver other messages that may be critical. Additionally, the receipt by College users of excessive numbers of mass emailing messages is a work-place irritant and does not promote the efficient use of information system or human resources.

Email does not include instant messaging (IM) capabilities.

Standards & Procedures:

Standards:

Attachment Type Limitations. Email attachments received on campus will be filtered to exclude specific filename extensions (e.g. .exe, .com) as may be determined to be a security threat by the College Information Security Officer.

Conveyance of Confidential or Sensitive Information. Users of all Email systems must be aware that information originated in or received through email messages is probably not encrypted and should not be considered as confidential or unaltered. Unencrypted email will not be used for the conveyance of personal or sensitive information (see Sensitive Information Protection Policy).

Email Broadcasts. Use of the centrally managed Email systems of the College for mass distribution of mailings will be governed by the criticality of the content of mailings as follows:

Critical Messages. Critical messages that need to be distributed to all College employees must be approved by the President, a Vice President, the Director of College Relations, or the Chief Information Officer prior to submission for distribution. Critical messages intended for students must be approved by the Vice President for Student Services prior to distribution. Critical messages are categorized as either *time-sensitive* or *non-time-sensitive*.

Informational Messages. Users of email systems at Darton College are not permitted to arbitrarily send messages to all, or nearly all, of the system users unless they are Darton College business

related. Instead, Luminis Groups have been created and are designed to reach targeted audiences. Individuals may selectively join any, or all, of these groups.

Email Relay. All College hosted email systems will be configured to prevent use by third parties as email relay platforms.

Email Systems. Office of Information Technology (OIT) will operate centrally managed email systems for the College to support the needs of faculty, staff, and students (and retirees as resources permit).

Passwords. Strong password guidelines as published in **Minimum Information Security Environment Policy** (Create or Change a Password) will be utilized on all College hosted Email systems.

Patch Management. Email servers must be updated with new security patches for both the operating system and mail server applications as those patches are released by vendors. OIT is responsible for patching the centrally managed email systems.

Student Email. All students registered for classes at Darton College are provided an email account through their access to the Darton College Campus Pipeline (MyDC) system. The College will use this email account to send communications to the student body. Student email addresses will be recorded in the College's electronic directories and records. Students are responsible for reading official College email in a timely fashion.

Virus Detection and Removal. Active anti-virus detection and quarantine clients will be installed on all email servers. Where possible, these anti-virus applications will be configured for automatic update of virus signatures. Additionally, anti-virus gateways will be utilized to scan inbound and outbound messages.

Information Systems Ethics Policy

POLICY:

Darton College's information system resources shall be made available only for appropriate uses, and will be used in a manner that protects both personal privacy and equitable availability across the College.

Rationale:

In order to further the College academic, research and service missions, a quality computing environment must be maintained. This environment ensures availability and equitable distribution of resources across the campus. Limited resources should not be used for purposes that are not directly related to the business of the College nor should they be used in a manner that would violate the personal privacy of faculty, staff or students associated with the College.

Standards & Procedures:

Standards:

Appropriate Use. Appropriate use of information systems is that which supports the College's objectives of teaching, research and extension of knowledge to the public.

Guidelines for the appropriate use of information systems:

a) Users shall not provide network or computer based services using College information systems without prior written approval and registration
b) Users shall not use information systems for promoting or maintaining a personal or private business or using College information resources for personal gain
c) Users shall not use information systems for unauthorized not-for profit business activities
d) Users shall not use information systems for creation, accession or transmission of pornographic, obscene, discriminatory, offensive, threatening, harassing, or intimidating materials
e) Users shall not use information systems for creation, accession, or participation in online gambling
f) Users shall not use information systems for activity or solicitation for political or religious causes
g) Users shall not use information systems to engage in harmful activities. Such activities include, but are not limited to, Internet Protocol (IP) spoofing, creating and/or propagating viruses, port scanning, disrupting services, damaging files, purporting or representing one's self as someone else, or intentional destruction of or damage to equipment, software or data.
h) Users shall not impede, interfere with, impair, or otherwise cause harm to other user's legitimate use of information systems
i) Users shall not use someone else's logon ID and password
j) Users shall not use information systems in such a way that violates local, state, or federal laws, including copyright, trademark, patent, or other intellectual property rights
k) Users shall be responsible for ascertaining that the use of information systems complies with all College policies
l) Users shall not use information systems in such a way that violates the College's contractual obligations, including limitations defined in software or other licensing agreements
m) Users shall not use information systems to transmit communications that are fraudulent,

defamatory, harassing, obscene, threatening, that unlawfully discriminate or that are prohibited by law

n) Users shall not modify or remove computer equipment, software or peripherals without proper authorization
o) Users shall not perform security scanning, probing or monitoring services without appropriate permission
p) Users shall not perform activities intended to circumvent security or access controls of any organization, including the possession or use of hardware or software tools intended to defeat software copy protection, discover passwords, identify security vulnerabilities, decrypt encrypted files, or compromise information security by any other means
q) Users shall not install or attach communication device(s) on computers or networks that allow off-campus devices to attach to the College network or computers without authorization
r) Users shall not disclose restricted College information
s) Users shall not engage in conduct that is inconsistent with the stated goals and mission of the College

College Access to User's Information (Privacy). College access to a user's information systems includes any access by the College to approach, enter, or make use of the information stored on the College's information systems. To the extent permitted by law, the College seeks to preserve an individual's information or data from unsanctioned intrusion. Electronic and other technological methods must not be used to infringe upon a user's privacy.

Guidelines concerning access to user information:

a) The College seeks to preserve individual privacy, and does not routinely monitor individual usage; however, the College may in accordance with state and federal law, access and monitor information systems when:
    1) the users has voluntarily made them accessible to the public
    2) It reasonably appears necessary to do so to protect the integrity, security, or functionality of the College or to protect the College from liability
    3) When necessary for the normal operation and maintenance of the information systems, or to identify or diagnose systems or security vulnerabilities and problems
    4) There are reasonable grounds to believe that a violation of law or a significant breach of College policy may have occurred
    5) An account appears to be engaged in unusual or unusually excessive activity as indicated by monitoring of general activity and usage patterns
    6) It is required by federal, state, or local law or administrative rules

b) Users understand that by attaching personal computing devices to the College information systems, they consent to the College's monitoring of their information systems for maintenance and security purpose

c) Users understand that by attaching personal computing devices to the College information systems, they consent to the College's monitoring of their information systems for maintenance and security purposes

d) Electronic mail messages are not secure and therefore should not be assumed to be private.

Procedures:
Request Authorization to Probe or Monitor College Information Systems

Request Authorization to probe or monitor College Information Systems

Procedures:

1. Obtain written approval from the individual whose information you wish to probe or monitor. Department Heads, or other appropriate positions of authority, may also grant permission to have an individual's information probed or monitored.
2. Inform the individual or Department head - in writing/email - of the specific time and date the investigation will occur.
3. Inform the individual or Department head - in writing/email - when the investigation is over.

Help:

If you have questions, or need assistance, please contact the Help Desk (229-430-6704 or helpdesk@darton.edu).

Internet Services (Server) Registration Policy

POLICY:

All devices connected to the Darton College network that are intended to "serve" information to on or off campus users must be registered with Office of Information Technology (OIT)
.

Rationale:

The rising frequency of security incidents involving network-attached devices significantly increases the probability of major disruptions to the internal computer systems of the College. Current server technology is easily implemented but the platforms if not properly configured provide an extremely vulnerable and high risk opportunity for exploitation and significant damage to other connected devices, other external devices, and other users. Registration of all such serving devices with accompanying procedures for verifying security configurations will significantly reduce the potential for this type of damage and also greatly shorten the time needed to identify and isolate equipment which has been inadvertently compromised. Additionally, care taken in build and deployment of serving devices provides a greater level of protection to other devices connected to the network. Establishing policy centrally and issuing standards and utilities from a central authority allows for rapid incident response and continuous update of protection methods.

Standards & Procedures:

Standards:

Compliance. Chairs and Vice Presidents are responsible for monitoring compliance with this policy and associated standards by: (1) directing the registration of machines within their respective organizations that meet the standard definition of servers; and (2) directing reviews of, and action on, reports on unregistered serving devices connected to the College network that are generated by OIT .

Definition of Servers. Typically, servers are machines that have intentionally been set up to provide services to others on campus or the Internet. These provided services could include Web (http) servers, FTP servers, file sharing servers, etc. Most of these services are not typically offered by end-user workstations. However, if an end-user workstation has installed or turned on web server, FTP server, etc. services, this machine would be required to register as a serving device.

Server Registration. As a minimum, OIT must be provided the following information on each device currently or intended to be attached to the College network for the purpose of "serving" information either on or off campus:

- Brand of hardware platform
- Operating system version
- Equipment MAC address
- Requested DNS name
- Assigned or requested IP address

- Person responsible for management of the device (including phone number and email address)
- Device physical location
- Internet services being offered by the platform
- Security Protection measures applied to the device

As a continuing activity associated with normal network management, OIT will periodically scan for network-connected devices. Any unregistered serving devices found during these scans will be isolated from the network until proper registration is accomplished. When it has been determined by the College Information Security Officer that a security incident or compromise has occurred, failure to have accomplished registration will result in deactivation of network ports associated with the serving device.

Server Security Audits. Administrative departments are responsible for developing and administering their own local procedures for initial verification of server security configuration as well as for ensuring that updated security patches are applied to serving devices within their respective organizations. Assistance from the College Network Support Specialist is available for initial system verification and for periodic scans of systems. OIT will provide minimum requirements for server configurations. Failure to meet these minimums will result in the serving device being isolated from the network.

Procedures:
Register an Internet Services (Server) Device
Ensure Currency of Patches for Internet Services (Server) Devices

Register, view, update, or delete existing information for Internet services devices attached to the University network.

About:

The **Internet Services Registration Policy** requires that Internet services devices (servers) be registered with Office of Information Technology. A server is defined as any device attached to the College network for the purpose of "serving" information either on or off campus. The registration process requires very specific technical information; therefore, it is suggested that each Department designate one or more technical staff members to register devices for their area.

Register a Device:

1. Complete the form “DNS Request” in Public Folders under Office of Information Technology.
   You will be contacted (usually within 24 hours) with your information.

Help:

If you have questions, or need assistance, please contact the Helpdesk (229-430-6704 or helpdesk@darton.edu).

Ensure that steps are taken to provide current security patches on server devices that are to be attached to the Darton College Network and the Internet.

Guidelines for Securing a Device to be Attached to the Georgia State Network and the Internet:

1. **Protect the device before it is attached to the network.**
   Devices can be compromised or infected with a virus within minutes of connection to the network. Do the following before attaching the device to the network:
   - Install current security patches for the device
   - Install anti-virus software
2. **Use Antivirus software.**
   Antivirus software is a necessity for windows operating system devices. Configure it to:
   - Scan for viruses in real time
   - Daily automatically update of virus signatures
   - Periodically perform a full virus scan of the device
3. **Shut down unnecessary services.**
   Disable services that are not required for the desired function of the device. Devices often come with many services enabled by default that are not necessary. Services that are not running cannot be used to penetrate the device.
4. **Install and configure a firewall.**
   A device may be protected by either an internal host based firewall or an external stand alone firewall. A firewall stance of "everything that is not explicitly denied is not allowed" is the industry best practice.
5. **Enable and enforce password standards.**
   Configure the device to require strong passwords. Enable as many of the following standards as possible:
   - Length of 6 characters or more
   - No word that can be found in a dictionary
   - A mixture of upper case, lower case, numerals and special characters
   - Password must be changed every 90 days
   - Passwords may not be reused
6. **Enable and configuring logging.**
   Typically, very little logging is enabled by default. Logging is extremely useful for detecting and unsuccessful and successful attempted penetrations.
7. **Stay up to date on security patches.**
   Security is an ongoing process. Apply security patches or workarounds promptly.
8. **Keep informed on security issues.**
   There are many security mailing lists and web pages available on the Internet. At a minimum, you should join the security alert mailing from the manufacturer of the network device if one is available. Here are links to sites for some major vendors as well as general security and antivirus information web sites. Many of these sites have mailing lists you may join to alert you to new security
9. **Vulnerabilities and patches**.

   - SANS – Sysadmin, Audit, Network, Security Institute
     http://www.sans.org
   - CERT – Computer Emergency Response Team Coordination Center
     http://www.cert.org
   - CIS - Center for Internet Security
     http://www.cisecurity.org

- Security Focus
  http://www.securityfocus.com
- Microsoft Security Information
  http://www.microsoft.com/security/default.asp
- Sun Microsystems Security Information
  http://sunsolve.sun.com/pub-cgi/show.pl?target=security/sec
- Apple Security Information
  http://www.info.apple.com/usen/security/index.html
- Linux Security Information
  http://www.linuxsecurity.com/

Help:

If you have questions, or need assistance, please contact the Help Desk (229-430-6704 or helpdesk@darton.edu).

Minimum Information Security Environment Policy

POLICY:

The College has both the right and the obligation to manage, protect, secure, and control the electronic information resources of the College.

Rationale:

The Director of Information Technology, as Chief Information Officer, is responsible for ensuring that Darton College has adequate information security in order for system and data to be available for appropriate purposes. The basic standards and guidelines described in this policy provide for the minimum acceptable environment for operating and accessing information systems.

Standards & Procedures:

Standards:

Authorized Access to Information Systems (Accounts). Authorized access to the College's information systems is the granting of authority to approach, enter, make use of, and exit the College's information systems. Access is accomplished via an account, which is a record kept by operating systems for each authorized user of information systems for the purpose of identification, administration and security. Users are required to obtain proper authorization prior to accessing the College's information systems.

Guidelines establishing eligibility to receive authorized access:

a) Every College employee or student eligible to register may be granted access to College information systems.
b) Users shall not be granted access in excess of the level required to perform their job responsibilities
c) Individuals providing services to the College may with appropriate authorization be granted access to College information systems
d) Users shall not misrepresent their identify or relationship to the College when accessing the information systems
e) Users shall not access information systems that they are not authorized to access

Configuration for Network Connection. Configuration refers to the version of operating system that is installed on your workstation, desktop or laptop computer. As each operating system version may handle other applications in a different manner, users must ensure that they check the current procedure for securing each device to determine the correct accompanying versions of Microsoft Servers, Exchange, AntiVirus and VPN client needed for access to the Darton Network. Users should be aware that a local decision to continue use of a non-supported version of operating system could result in denial of network connection due to increased risk of new security holes that will not be addressed by the software vendor.

Passwords and Userids (Authentication Methods). A userid and password is one method (and the one most commonly recognized by the average user) of authentication. A userid is the name by which the person is known and addressed on the College's information systems. The password – used in conjunction with the userid – is a unique string of characters that a user enters as an identification code. Users must follow standards for creating passwords as defined in the "Create or Change a Password" document (see link in **Procedures** section). Other recognized forms of authentication include, but are not limited to, smart cards, swipe cards, one-time passwords, digital signatures, and/or digital keys and biometrics. Users must have a valid method of authentication before they will be authorized to access the information systems.

Guidelines regarding the use of userids and passwords:

a) Users must not use accounts or passwords that they have not been authorized to use, or have not been assigned to them
b) Users shall not give passwords to unauthorized users
c) Users shall not share userids and passwords
d) Users must effectively control the creation, use and maintenance of passwords in order to prevent unauthorized access and destruction, modification or deletion of sensitive data
e) Users are responsible for securing their passwords from inadvertent disclosure
f) Users are responsible for any activity carried out under their account identification.

Software Licensing. Valid licenses are required for each end user for all commercially developed software operating on systems used by that user. Responsibility for centrally managed and distributed software lies with OIT. Departments are responsible for approving and retaining documentation on software (other than centrally managed) installed on devices within their areas of responsibility. As a minimum departments should be able to show original licensing materials (packaging, hologram software seal, authorization codes, etc.), date of installation and serial number of equipment (or Darton Inventory number) that the software was installed on. Departments are responsible for developing and managing their own procedures for collecting and maintaining licensing records. All students and personnel shall abide by software copyright laws and shall not obtain, install, replicate, or use software except as permitted by the software licensing agreements.

Using Personally Owned Software. To protect the integrity of the College information resources, students and personnel shall not use personally owned software on College owned equipment. This includes purchased and licensed applications; shareware; freeware; downloads from bulletin boards, Internet, Intranet, FTP sites, local area networks (LANs) or wide area networks (WANs); and other personally-owned or controlled software (unless otherwise authorized by the Chief Information Officer or his / her designees).

Physical Security. Physical security refers to the protection from harm or loss of the pieces of equipment that constitute an information system environment or personal computing device. Information system must be safeguarded in a way that minimizes the risk of abuse, theft and destruction.

Guidelines regarding physical security:

a) Users must implement appropriate protection measures including physical barriers, environmental detection and protection, insurance, and/or other risk management techniques.
b) Users must not leave mobile computer systems unattended for extended periods of time and shall utilize locking devices responsibly
c) Users shall protect information systems by utilizing protective measures such as locked screens and password-protected screen savers.

Securing College Information Systems. Securing systems refers to the protection of a computer system and its data from harm or loss, particularly the prevention of access by unauthorized individuals. Users are responsible for properly securing their information systems.

Guidelines for securing systems:

a) Users shall not knowingly defeat or attempt to defeat the security of information systems
b) Users must take reasonable precautions in ensuring that they do not disseminate viruses and malicious programs to other users
c) Users must configure College mail servers to prevent them from being used as third party mail relays
d) Users are responsible for monitoring the security of their own information systems
e) Users who are permitted to provide network or computer based services are required to take reasonable precautions to ensure that information systems being used for this purpose are not compromised or used by unauthorized users. See Sensitive Information Protection Policy for guidelines.

Chief Information Officer (CIO). The Chief Information Officer (CIO), Director for Information Technology, has responsibility for developing and publicizing College information security policies as well as monitoring compliance with those policies and all applicable laws, rules and regulations. The CIO coordinates the standards, procedures and guidelines necessary to administer access to College information resources. The CIO works in conjunction with information resource owners, the College Data Administrators, and functional users to develop this material.

Procedures:
Create or Change a Password
Request Access to College Restricted Data
Secure Your Workstation – In development for web

Create or Change a Password

Guidelines for choosing strong passwords, instructions for changing passwords (Windows Workstations and MyDC Accounts), installing a screen password, and requesting a password reset.

About:

A password is your system's - and the College network's - security. As well as protecting your own system, securing your personal computer from outside intrusions minimizes attacks on the University network. Many attacks on personal computers are simply an attempt to locate an "entrance" into the larger College network. If an attempted attack on your machine is unsuccessful, not only have you thwarted a local intrusion, more than likely, you've protected the College network as well. Therefore, protect your computer - as well as the entire College network - by choosing a strong password for your personal computer, and changing it frequently.

Important **- Guidelines for Creating Secure Passwords:**

Passwords should:
- be at least six characters long; generally, no more than eight
- consist of mixed case (at least one each of upper and lower case)
- contain at least one non-alpha character (such as a number or symbol)
- be different for different systems - especially for Darton versus non-Darton systems
- be changed frequently

Hint: A strong password might look something like: **wh3WdhG1**

Passwords should ***not***:
- be a name (pet, family member, friend, etc.)
- contain personal information that others would know about you
- be a word that can be found in the dictionary

NOTE:
Passwords are usually configured to expire every 90 days. At the time of expiration, you will receive a notice that your password has expired and you will be prompted to change it.

Change Windows NT/2000/XP and Exchange email passwords:

1. Press **Control/Alt/Delete.**
2. Click **Change Password.**
3. Enter your **old password**, you **new password**, and then your **new password** a second time.
4. Click **OK**.

Change MyDC Passwords:

1. Login to Banner Web through the Luminis Portal.
2. Enter **passwd** at the prompt.
3. Enter your **old password** at the next prompt
4. Enter a **new password** twice as prompted.

Install a Screen Password:

1. Click **Start**.
2. Click **Settings**.
3. Click **Control Panel**.
4. Click **Display**.
5. Click the **Screen Saver** tab.
6. Click the **drop-down box arrow**, and then choose a **Screen Saver**.
7. Click the **Settings** tab.
8. Check the **Password Protector** box.
9. Fill in **Wait X minutes** (This is the number of minutes you want the computer to wait before displaying the screen saver.)

Help:

If you have questions please contact the Help Desk for assistance (229-430-6704) or helpdesk@darton.edu).

Network Connections for Surveillance System Cameras and Digital Video Recorders Policy

POLICY:

The Darton College network infrastructure may serve as a distribution means for digital information collected by surveillance camera systems and associated recording devices that are primarily used for obtaining identifiable personal images. Connection of IP addressable cameras and digital video recorder systems used for this purpose to the Darton College network (either through direct copper/fiber wiring or indirect 802.X technology) must be approved by the College Chief Information Officer (CIO) and the Network Support Specialist prior to being placed in operation.

Rationale:

Increased attention to security and protection of human and physical resources around the Darton College campus has resulted in need for quickly deployed and easily maintained security and surveillance systems. Digital recording devices and digital monitoring devices provide a very cost effective solution and are readily available. However, placing these devices on the data network without proper information security consideration or configuration could result in access to the system or to information being collected on the system by unauthorized users. This is particularly critical for systems that are either protecting valuable resources or for systems that may collect evidentiary information for future prosecution of suspects. In order to ensure systems are being accessed only by the minimum persons required, equipment and software must be reviewed by the CIO and network staff to determine if the requested system can be secured, methods that can be used to access the system from on and off campus, and potential impact on network traffic when the system is placed in service.

Standards & Procedures:

Standards:

Denial of Access. IP addressable cameras and IP addressable digital video recorders (DVR) (associated with either analog or digital cameras) making a physical or 802.X connection to the College network infrastructure must allow for denial of access by other than those users specifically included in a system Access Control List (ACL).

Access through VPN. All access to IP addressable cameras and associated digital recorders used for security and surveillance from other than physical connections to the campus network will be accomplished through the centrally managed Virtual Private Network (VPN).

Audit Reporting of Accesses. Digital video recorders used to collect and store identifiable personal images should be configurable to allow audit reporting of accesses to the recorder.

Evidentiary Documentation. Digital video recorders used to collect and store identifiable personal images should include technology for “watermarking” of files in order to be suitable for evidentiary documentation.

Systems Accesses by Darton Policy Personnel. Security and surveillance camera systems that are intended to be accessed by Darton College Security personnel will comply with the following technical specifications:

- Allow for simultaneous viewing of live and recorded images
- Store recorded images in MPEG II format
- Include capability for transfer of stored images to external storage media
- Does not require vendor specific/proprietary applications or clients for viewing live or stored images
- Provides 7 days of image storage from all connected cameras on the recording device

Procedures:
Request Assistance with Requirements for Security Control or Surveillance Systems
Request Review and Approval of Selected Surveillance Systems Prior to Installation
Register Internet Services Devices (Servers)
Digital Video Recorders are classified as "servers" and must be registered in accordance with College Policy.

Remote Access Policy

POLICY:

Remote connection to Darton College's computer systems, networks, and data repositories will be permitted only through secure, authenticated, and centrally managed access methods.

Rationale:

Increases in non-traditional teaching methods and the increased mobility of faculty and students has made remote access to centralized College assets increasingly important. Opening uncontrolled or unsecured paths into any element of the College network or internal computer systems presents additional risk to the entire College infrastructure. Establishing policy centrally and issuing standards from a central authority allows a minimum number of penetrations of the security of the network while still allowing flexibility in the actual remote connection technology used.

Standards & Procedures:

Standards:

Office of Information Technology (OIT), as the manager of the institutional infrastructure, will establish and publish standards after coordination through the Information and Instructional Technology Committee. College and Departmental IT contacts will provide recommendations to OIT for the development of standards and will assist with monitoring compliance with the standards by their respective users. Changes to standards when necessary will be communicated to the College by OIT.

Access to single host systems. Remote access to single equipment hosts (i.e. departmental servers, WEB hosting equipment) is permitted by following these standards:

- Departmental host may provide dial-up modem service ONLY IF that service is limited exclusively to College members and the host prevents connection to the Darton College network for those dial-in users.
- WEB hosting servers may provide anonymous or authenticated access to pages ONLY IF the service host prevents an onward unauthenticated connection to the Darton College network.

In both instances, departments are responsible for hosts/servers operating within their departments.

Administration/Authentication. The administration and authentication system for remote access will be centrally managed.

Affiliates are personnel that are not faculty, staff or students at the College who require remote access privileges. Affiliations may be requested by faculty and staff and are subject to an approval process. Affiliations are valid for a maximum of six months and are renewable.

Authentication for remote access will be strong. Passwords will not traverse the network in the clear text and must meet minimum requirements as documented in College security policies.

Anonymous Interaction. With the exception of web servers, electronic bulletin boards, or other systems where all regular users are anonymous, users are prohibited from remotely logging into any Darton College system or network anonymously (for example, by using "guest" user-IDs). If users employ systems facilities which allow them to change the active user-ID to gain certain privileges, they must have initially logged-in employing a user-ID that clearly indicates their identity.

Anti-Virus and Firewall Protection. External computers or networks making remote connection to College internal computers or networks must utilize an active virus scanning and repair program and an active personal firewall system (hardware or software).

Default to Denial. If a College computer or network access control system is not functioning properly, it must default to denial of access privileges to users. If access control systems are malfunctioning, the systems they support must remain unavailable until such time as the problem has been rectified.

Disclosure of Systems Information. The internal addresses, configurations, and related system design information for Darton College computers and networks is confidential and must not be released to third parties who do not have a demonstrable need-to-know such information. Likewise, the security measures employed to protect College computers and networks are confidential and should be similarly protected.

Failure to Authenticate. All systems accepting remote connections from public network connected users (users connected through dial-up phone modems, Internet Service Providers, or cable modems) must temporarily terminate the connection or time-out the user-ID following a sequence of several unsuccessful attempts to log-in. For example, if an incorrect dynamic password is provided three consecutive times, dial-up systems should drop the connection. Repeated unsuccessful attempts to remotely establish a connection using a privileged user-ID must not result in the revocation (suspension as opposed to time-out) of the user-ID because this could interfere with the ability of authorized parties to respond to security incidents.

Initiating Remote Sessions. Instruction and assistance on initiating remote access sessions will be developed and offered by Departmental IT contacts in coordination with OIT.

Management Consoles and Other Special Needs. Users requiring modem access for “out of band” management or special needs must register the modem and its use with OIT. Each registration is approved on an individual basis. Any dialup server that grants network access must authenticate each user, minimally by a unique identification with password and should encrypt the data stream. All calls are to be logged and logs of access should be retained for 30 days. At the completion of each dialup session to a server, the accessing workstation will be secured via password.

External Agency Systems: Any external system hosted on the Darton network is subject to the standards and procedures written and used to implement this policy.

Modems on Desktop Systems. Existing modems in or connected to campus LAN connected desktop PCs that are used for remote control and file transfer from a remote location to those desktops are to be phased out in favor of a secure TCP/IP or VPN connection. In the interim, users must use OIT approved software to establish a remote connection through an ISP, modem bank or the network to terminate at the host campus computer with a secure connection. Home-based, handheld, mobile and/or telecommuting microcomputers used exclusively off-campus are

exceptions to this rule. Unless a dynamic password system is installed, workers with home based, mobile, or telecommuting PCs must not leave modems in auto-answer mode, with communications software enabled, such that in-coming dial-up calls could be received.

Privilege Access Controls. All computers permanently or intermittently connected to either external networks or College networks must operate with privilege access controls approved by the Office of Information Technology. Multi-user systems must employ user-IDs unique to each user, as well as user privilege restriction mechanisms including directory and file access permissions. Network-connected single-user systems must employ approved hardware or software mechanisms that control system booting and that include a time-out-after-no-activity screen blanker.

Remote Access to College Information. Systems that contain confidential student, personnel and financial data will be available for off-site remote access only after an explicit request is made and approved by the data steward for the target system. Access will be permitted through a centrally managed virtual private network (VPN) that provides encryption and secure authentication. Access may be revoked at any time for reasons including non-compliance with security policies, request by the user's supervisor or negative impact on overall network performance attributable to remote connections. Remote access privileges for College Information will be reviewed upon an employee's change of departments.

Time-Out. All systems accepting remote connections from public network connected users (users connected through dial-up phone modems, Internet Service Providers, or cable modems) must include a time-out system. This time-out system must terminate all sessions that have had no activity for a period of 30 minutes or less. An absolute time-out will occur after 24 hours of continuous connection and will require reconnection and authentication to re-enter the network. In addition, all user-IDs registered to networks or computers with external access facilities must be automatically suspended after a period of 30 days of inactivity.

Procedures:
Access Darton's Network via Virtual Private Network

Reporting and Handling Security Incident Response Policy

POLICY:

Full Policy is in development. The Darton College Technology Incident Report Form has been in use for several years.

Rationale:

Standards & Procedures:

Standards:

Procedures:

Within 30 minutes of incident, the Darton College Technology Incident Report should be completed and reported to one of the individuals listed on other side. If incident occurs after hours page one of the individuals and they will make a decision regarding escalation. If appropriate, OIIT will be notified. Additional Sheets may be attached as needed.

DARTON COLLEGE TECHNOLOGY INCIDENT REPORT

Office of Information Technology (OIT)

		Emergency Contact Pager
TO:	Margaret Bragg, Director, OIT/CIO	229-878-3688
	Brian Anderson, Systems Analyst II/DBA	229-434-3603
	Ashley Coates, Network Analyst	229-878-3681
	Michael Johnson, Systems Administrator/Help Desk Manager	229-434-3015

Personnel Reporting Incident: _____ DATE_____

Location: _____

Time: _____ a.m./p.m. Security Called? Yes No
Police Called? Yes No

Summary: _____

_____

_____

_____

_____

Name(s) of person(s) involved (including witnesses)	- Student: ID Number - Employee: Department - Visitor	Other Information (Relative, telephone number, etc)

OIT Personnel must complete other side of this form for report to be complete Revised: 09/03

This is an: _____ Initial Report: _____follow-up report

_____

Details of Incident: _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Follow-up Required? By Whom? _____

_____

_____

_____

OIT Personnel Name (Print) _____

OIT Personnel Signature _____

Date: _____

Within 30 minutes of incident, this report should be completed and reported to one of the individuals listed on other side. If incident occurs after hours page one of the individuals and they will make a decision regarding escalation. Additional Sheets may be attached as needed.

Sensitive Information Protection Policy

POLICY:

Information systems storing or serving sensitive information should be operated on secured systems within the environment of the Office of Information Technology (OIT).

Rationale:

The rising frequency of security incidents involving network-attached devices significantly increases the probability that sensitive data if not properly authorized and protected may be exposed to unauthorized viewing or modification. Addressing the potential of identify theft of information about individuals has become an increasing concern of the institution. Established procedures for protection and release of sensitive information must be followed regardless of the platform that data is being stored or processed on.

Standards & Procedures:

Standards:

Compliance. Chairs and Vice Presidents are responsible for monitoring compliance by their respective users with this policy and associated standards by: (1) directing compliance with the Internet Services Registration policy; and (2) directing reviews of, and action on, reports on compliance with this policy that are generated by the Office of Information Technology (OIT).

Sensitive Information on Serving Devices. Sensitive Information is defined as any combination of the following data records:

- Social Security Account Number
- Personal identification numbers which may be used other than Social Security Number
- Information protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Information protected by the Family Educational Rights and Privacy Act (FERPA)
- Credit card account numbers
- Bank account numbers
- Lists of computer systems ids and/or passwords

The Darton College Data Stewardship and Access Policy for College Information specifies policy regarding propriety and coordination of both accessing and sharing of institutional information by faculty and staff. The Designated Data Steward for the particular data in question is defined in that policy as the person responsible for delegating authority for viewing and sharing such information.

Sensitive Information on Desktops/Laptops/Workstations. Storage of sensitive information on devices that are not used or configured to operate as serving devices is acceptable if the user responsible for the device takes proper care to isolate and protect files containing that information from inadvertent or unauthorized access or viewing. Assistance with securing sensitive information may be obtained from the Office of Information Technology.

Alternative Locations for Serving Devices. Alternative locations must be reviewed and approved by the Chief Information Officer. Such exceptions will be made only after it has determined that the server providing sensitive information to the campus network and/or to the Internet is secured through reasonable procedures.

Procedures:
None

Student Computer Access Policy

POLICY:

All students must have access to a computer, and any course offered at Darton College may require computer-based work. It is the responsibility of students to ensure their access to computers. Departments and other units may establish minimum machine and software requirements, including the requirement to own a computer, for students in their degree programs.

Rationale:

Computer literacy and appropriate use of information technology is a central component of current academic policies. This policy does not require all students to own computers since the open access labs will provide the necessary basic capabilities.

Standards & Procedures:

Standards:

Computer Configuration. Computers that students have access to must provide access to web-based email accounts, the worldwide web using a current browser, spreadsheet capability and word processing. The Office of Information Technology will establish minimum equipment and software requirements.

Procedures:
None

Wireless Access Policy

POLICY:

Authorized users of Darton College computer systems networks and data repositories may be permitted to use wireless technology to connect to those systems, networks or data repositories to conduct College related business only through authenticated and centrally managed access methods.

Rationale:

Increase in the availability of wireless technology and the ease of deployment has significantly increased the potential for unauthorized access to College information systems. Deployment of the Wireless system established a framework for authenticated access across the campus. Establishing policy centrally and configuration and management of access points by a central authority allow a minimum number of penetrations of the security of the network.

Standards & Procedures:

Standards:

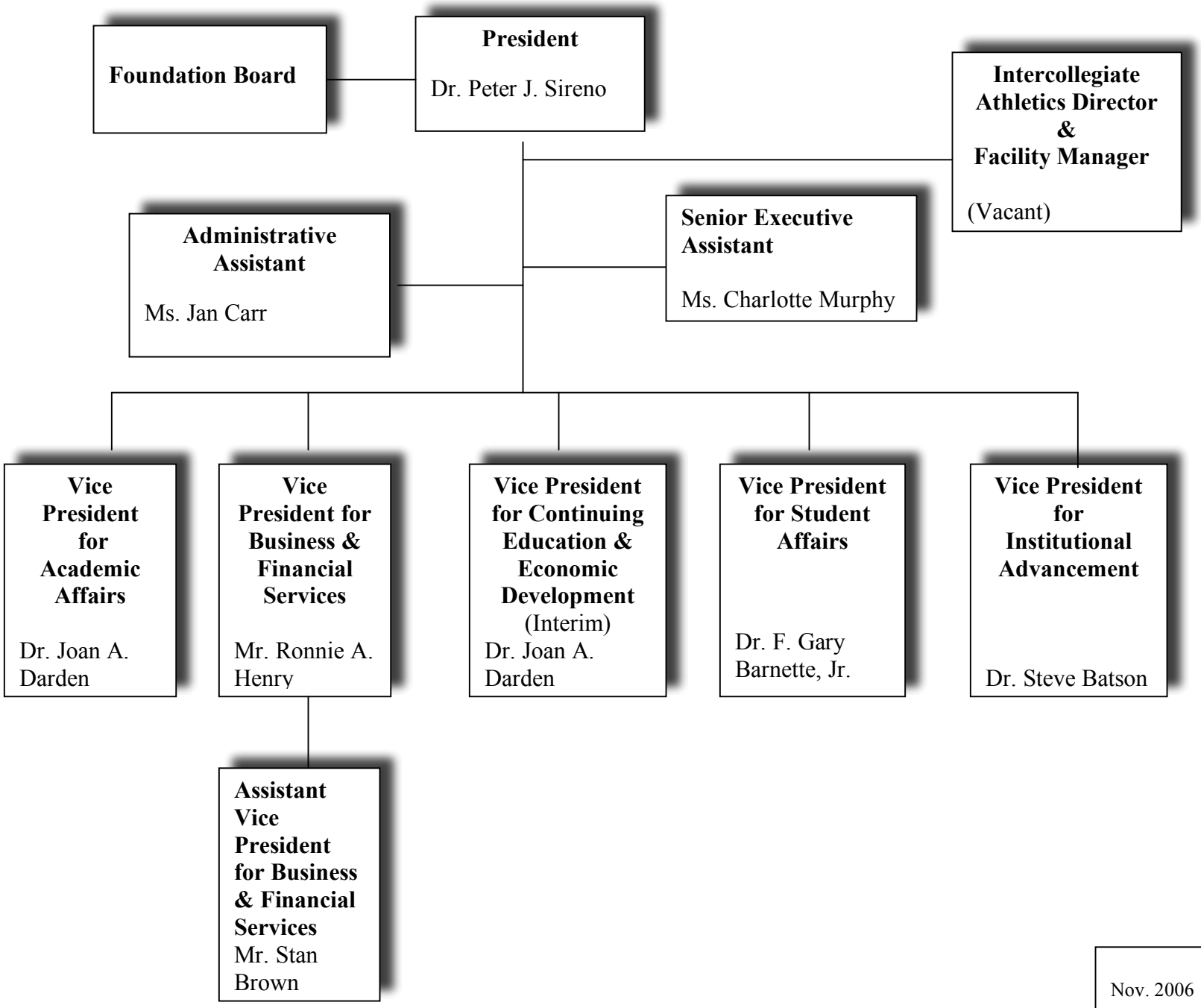
Access Method. All access through wireless access points connected to the College network infrastructure (regardless of duration) will be by Secure WEP and authenticated using userid and password. Mobile access points will be permitted to operate only from network ports configured by the Office of Information Technology (OIT) for this purpose.

Configuration, Installation, and Management. All fixed wireless access points connecting to the College network infrastructure will be configured, installed and managed by OIT. Existing access points must, as a minimum, provide 802.11b service and be configurable to block broadcast of SSID.

Unauthorized Access Points. OIT will periodically check the campus for unauthorized fixed and mobile access points, immediately disable the network ports supporting those access points and advise the operating department of necessity to comply with this policy.

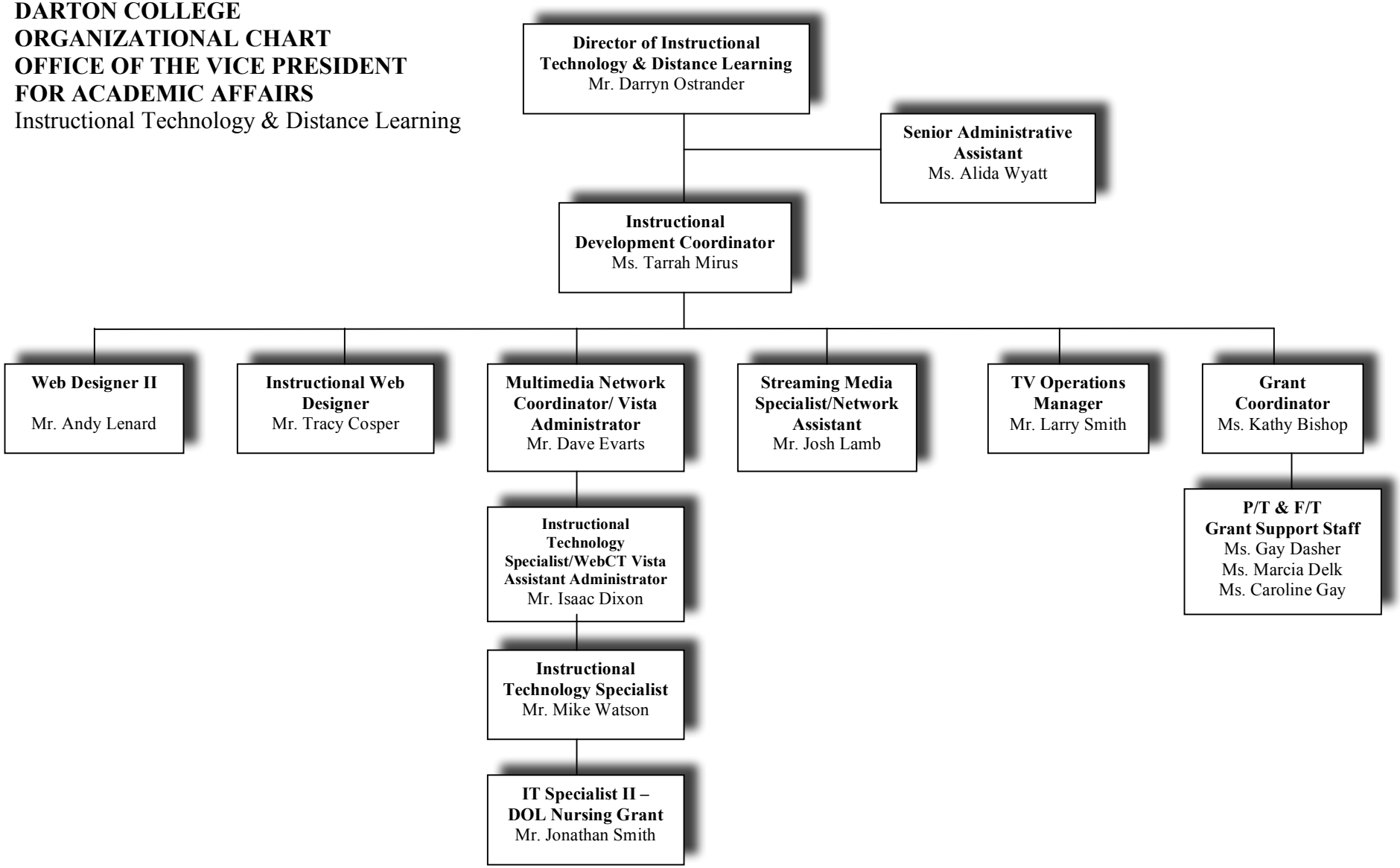
Procedures:
Access Darton College's Network via Wireless Connection

DARTON COLLEGE
ORGANIZATIONAL CHART
OFFICE OF THE PRESIDENT



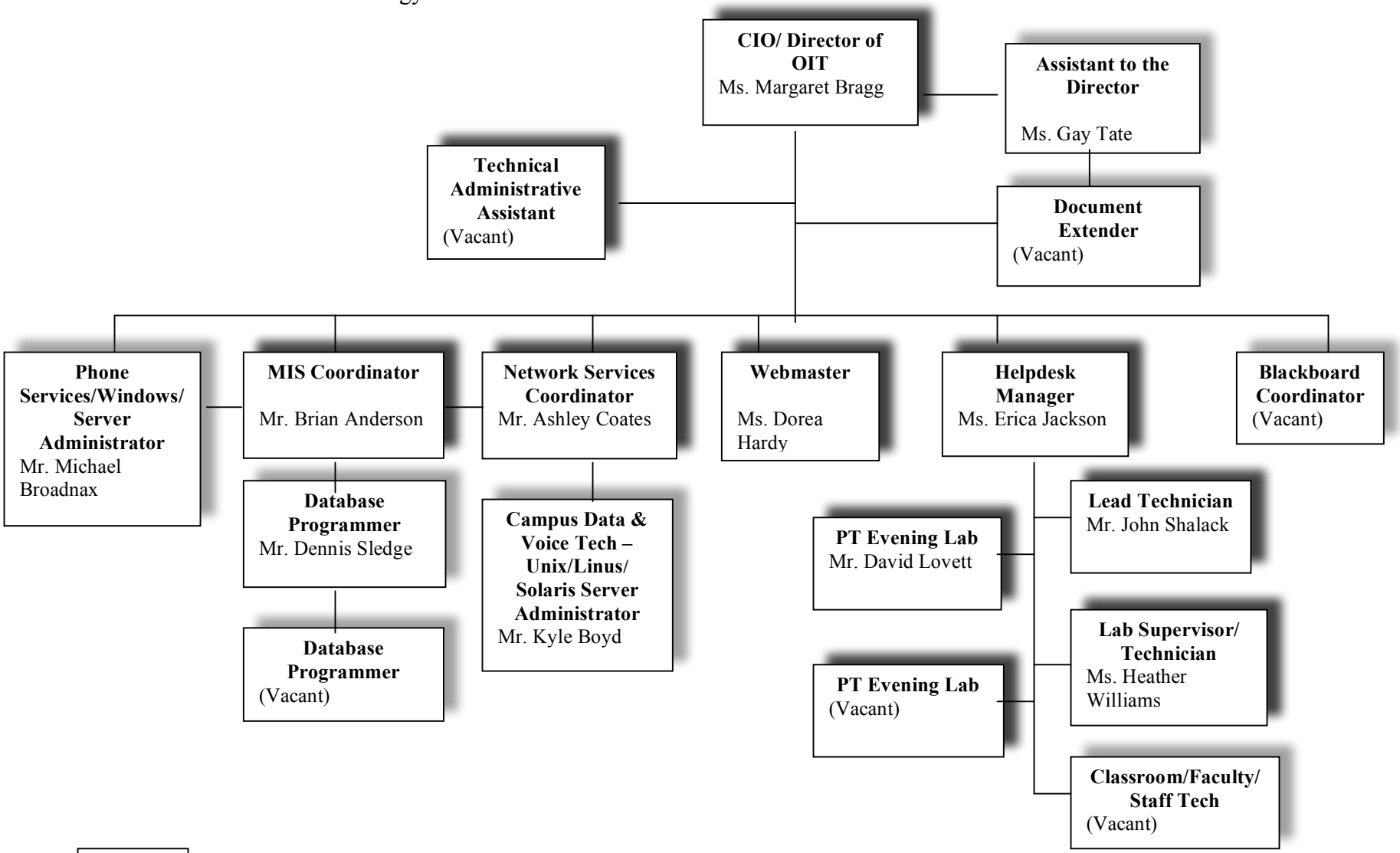
Nov. 2006

DARTON COLLEGE
ORGANIZATIONAL CHART
OFFICE OF THE VICE PRESIDENT
FOR ACADEMIC AFFAIRS
Instructional Technology & Distance Learning



July 2007

DARTON COLLEGE
ORGANIZATIONAL CHART
OFFICE OF THE VICE PRESIDENT
FOR BUSINESS AND FINANCIAL SERVICES
Office of Information Technology



Nov. 2006

Critical Server Assets

Host	Make/Model	Domain	Function
T188-101433	PowerEdge 2300/450	dc.edu	Domain Controller, DNS, WINS for Windows 2000 domain **dc.edu**.
IRIS	PowerEdge 1550/1000	dc.edu	Web reporting (web.darton.edu)
T188-102978	PowerEdge 1650	dar.dc.edu	Domain Controller, DNS, WINS for Windows 2000 domain **dar.dc.edu**.
T188-102775	PowerEdge 2550	dar.dc.edu	Banner forms, PeopleSoft forms, Bank reconciliation, Financial Aid, Foundation
T188-102776	PowerEdge 2550	dar.dc.edu	OIT Helpdesk application server
T188-101428	OptiPlex GX400	dar.dc.edu	OIT application storage server, image storage server
T188-103179	PowerEdge 1750	dar.dc.edu	User storage server
J131-103216	PowerEdge 2650	dar.dc.edu	Backup Real Server
J131-102732	PowerEdge 4600	dar.dc.edu	Backup support online courses and campus support
J131-100721	PowerEdge 4300	dar.dc.edu	Backup webpage support for online courses and distance learning
J131-103215	PowerEdge 2650	dar.dc.edu	Audio and video support for online courses and distance learning
J131-102731	PowerEdge 4600	dar.dc.edu	Online courses and campus support
J131-100720	PowerEdge 4300	dar.dc.edu	Webpage support for online courses and distance learning
T188-103181	PowerEdge 1750	dc.darton.edu	Domain Controller, DNS, WINS for Windows 2003 domain **dc.darton.edu**.
T188-359383	HP Proliant DL360	dc.darton.edu	Backup server
T188-101432	PowerEdge 7500	dc.darton.edu	Windows System Update Services server
T188-101029	OptiPlex GX400	dc.darton.edu	McAfee e-Policy server
T188-103241	Visual Sentry	dc.darton.edu	Surveillance camera server
T188-103242	Visual Sentry	dc.darton.edu	Surveillance camera server
T188-103180	PowerEdge 1750	acad.dc.darton.edu	Domain Controller, DNS, WINS for Windows 2003 domain **acad**.**dc.darton.edu**.
CORDELE-P7802	OptiPlex GX400	acad.dc.darton.edu	Cordele DHCP server, Banner forms for Cordele fac/staff
T188-101317	OptiPlex GX1	acad.dc.darton.edu	Compass Testing server
T188-103207 *(dc)*	PowerEdge 1750	dar.dc.darton.edu	Domain Controller, DNS, WINS for Windows 2003 domain **dar**.**dc.darton.edu**.
T188-103234	PowerEdge 2650	dar.dc.darton.edu	Exchange Server 2003

Host	Make/Model	Domain	Function
www.darton.edu	PowerEdge 1750	darton.edu	WWW (Darton homepage)
ns1.darton.edu	PowerEdge 1550	darton.edu	DNS, DHCP, NTP
ns2.darton.edu	PowerEdge 1550	darton.edu	DHCP
mxgw01.darton.edu	OptiPlex GX270	darton.edu	Mail/virus scanning gateway
mxgw02.darton.edu	OptiPlex GX270	darton.edu	Mail/virus scanning gateway
Gaia	HP9000 / N4000	darton.edu	Production databases, backup server
Dcban	HP9000 / K460	darton.edu	Test / Development databases
Cavalier	HP9000 / G40	darton.edu	Foundation data
Eros	Sun E250	darton.edu	CGP, Banner SS
lumtest	Sun E250	darton.edu	Test / Development Banner SS, Luminis test install, Test INB
lum1	Sun V440	darton.edu	Luminis (MyDC) web server, calendar Server
lum2	Sun V240	darton.edu	Luminis mail server
lum3	Sun V240	darton.edu	Luminis database server
J131-100726	PowerEdge 4300	none	none
J131-100722	PowerEdge 4400	none	none
J131-100724	PowerEdge 4300	none	Webpage support for Grant Funded Programs
J131-100723	PowerEdge 4300	none	none

Physical Hazards

Most equipment is located in Darton's central network and computing facility, located in the Administration Building. There are two entrances to this room, both keyed the same; this room is not on the master key system for Darton. The central computer room, storage room, and the Director's Office are on a separate key system, and maintenance, security and janitorial services do not have access to these areas. Keys for these areas are limited to designated computer personnel.

Temperature and humidity are controlled using a central air conditioning system located in the central network and computing facility.

A fire extinguisher is located inside the central computer room as well as in the adjoining room (A-198). A fire alarm pull box is located outside the central computer room.

All the critical equipment is protected by vendor maintenance contracts.

The servers for on-line classes, managed by the ITDL department, are located in J-131. This is a secured room with limited access. A fire extinguisher is located outside this room. There is a separate air conditioning unit for this room.

Access Control

Access to systems varies widely, based upon the nature of the system, and the services provided. The most restricted access policies exist on the administrative systems and include administrator (root) access to all critical systems. User access to systems like < >, which provides access to all college personnel, is much less restricted.

Gaia Dcban Cavalier	Accounts are established on a need only basis. Access is granted by the appropriate Systems/Database Administrator. User IDs have expiring passwords, forcing periodic change. Passwords have a minimum length. Passwords are stored in an encrypted form. Accounts are deleted when the user is no longer employed by the College. If the employee changes positions, all access rights are reviewed and adjusted as necessary.
T188-101433 T188-103181 T188-103182	Accounts are established on a need only basis. Access is granted by the appropriate Systems/Database Administrator. Passwords have a minimum length. Passwords are stored in an encrypted form. Accounts are deleted when the user is no longer employed by the College.
T188-102978 T188-103207 T188-103234	Accounts are established for all employees. Access is granted based upon a request from the user's department. Passwords have a minimum length. Passwords do not expire. Accounts are deleted when the user is no longer employed by the College.
T188-103180	Accounts are established individually for all students.
Administrator (root) access for all systems	Access to systems as administrator or root is strictly controlled. Only those people who have responsibility to administer or work on the systems are granted this access. Requirements are as follows: Accounts are created by the appropriate Systems/Database Administrator by request only. Access is granted only to the systems or areas of the systems which are needed. User IDs have expiring passwords, forcing periodic change. Usage of user IDs is logged and monitored. User IDs are deleted when they are no longer needed. All systems administrators have normal, non-privileged user IDs and are directed to use these for normal, day-to-day work. The administrator or root ID is only used when required.

All systems store the password in an encrypted form. This prevents anyone from ever knowing the original password. In the event of a forgotten password the administrator for a given system will change it to a known value and give this new value to the user. Most systems then set this new value as expired and require the user to change it again the first time they access the system using the new password. In the event a password is compromised or believed to be compromised, the standard procedure is to immediately deny access to that system for that account. This is to prevent further damage to the system. The administrator responsible for that account will conduct an investigation and the appropriate measures taken to ensure that the new password will not be compromised.

DARTON COLLEGE

Information Technology Security Policy

December 2007

INFORMATION TECHNOLOGY SECURITY POLICY

TABLE OF CONTENTS

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 polices, 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 6 and 8 alphanumeric characters long minimum
- 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 90 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.

<u>Darton College Faculty/Staff Workstations</u>

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.