



Information Systems Use Policies

March 31, 2009

2400 Gillionville Road
Albany, GA 31707
(229) 317-6704
(226) 317-6604 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.

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 promote 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	<p>Minimum precautions for securing computing devices and access to the Darton network. Responsibilities of the Information Security Officer.</p>	<p>Anyone at Darton using computers or having responsibility for a server</p>	<p>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.</p>
Network Connection of Surveillance System Cameras and Digital Video Recorders Policy	<p>Approval and configuration requirements for video systems used to protect resources or personnel.</p>	<p>Anyone at Darton planning to install a digital surveillance system</p>	<p>Contact the Chief Information Officer prior to acquisition and installation.</p>
Remote Access Policy	<p>Off-campus access to network and systems are through approved methods only.</p>	<p>Anyone at Darton providing access to local servers from off-campus locations</p> <hr/> <p>Anyone accessing a Darton network or information system from off-campus</p>	<p>Read the policy and follow the outlined standards and procedures.</p> <hr/> <p>Use a Virtual Private Network (VPN) client for authentication and encryption; see Procedure for details.</p>
Reporting and Handling Security Incident Response Policy	<p>Steps for reporting and handling security incidents.</p>	<p>Anyone at Darton using computers or have responsibility for security.</p>	<p>How to report an incident. How to manage incidents. Collection and sharing of information guidelines.</p>
Sensitive Information Protection Policy	<p>Protection of systems holding Social Security Numbers, credit card numbers, and other identity or personal information.</p>	<p>Anyone at Darton storing identity or personal information about other people on desktops or servers</p>	<p>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.</p>

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"