

Delgado Community College

Information Technology
Security Policy

Approved: November 5, 2010

Table of Contents

Title	Page
1.0 Introduction	5
1.1 Purpose	5
1.2 Management's View and Enforcement of Security	5
1.3 Security Policy Objectives and Methods	5, 6
2.0 Security Personnel	6
2.1 Chief Information Security Officer	6
2.2 Internal Controls Administrator	7
2.3 Security Analyst	7
2.4 Network & Communications Services Manager	7
3.0 Electronic Mail (E-mail)	8
3.1 E-mail Purpose	8
3.2 E-mail Privacy	8
3.3 E-mail Usage	8, 9
4.0 Internet Usage	9
4.1 Proper Internet Usage	9, 10
4.2 Wireless Access	10
5.0 Software	10
5.1 Downloading and Installing Software	11
6.0 End-User Account Access	11
6.1 Account Creation	11, 12
6.2 Account Logons and Passwords	11, 12
6.3 Password Selection and Management	12, 13
6.4 Temporary or Contracted Employees	13
6.5 Account Modification	13
6.6 Account Removal	13, 14
6.7 Remote Access	14

Table of Contents

<u>Title</u>	<u>Page</u>
7.0 Physical Controls	14
7.1 O.I.T. Area - Physical Controls	14
7.2 Computer Theft	14
7.3 Locks	15
7.4 Portable Devices	15
8.0 Security and Responsibilities	15-17
9.0 Virus Detection Software	18
10.0 Social Engineering	18, 19
11.0 Privacy of Students	19
12.0 Telecommunications	19, 20
13.0 Confidentiality	20, 21
14.0 Data Sanitization	21
15.0 Data Security	21
15.1 Data Security – Backups	21, 22
15.2 Data Security – Auditing and Monitoring	22
15.3 Data Security – Encryption	23
15.4 Data Security – Retention and Compliance	23
16.0 Reporting Violation Incidents	23
16.1 Technology Security Violations	23

Table of Contents

<u>Title</u>	<u>Page</u>
17.0 O.I.T. Internal Process for Acquiring Services	24
17.1 Network and Mainframe Access	24
18.0 Policy Development, Approval and Implementation	25
19.0 Acknowledgments	25
20.0 Cancellation	25
Glossary of Terms	26, 27
Administrative Systems Data Managers	28
Faculty/Staff Email Accounts	29

1.0 Introduction

Today, information technology (IT) permeates all aspects of teaching, learning, research, outreach, and the business and facilities functions of the College. Safeguarding information and information systems is, therefore, essential to preserving the ability of the College to perform its missions and meet its responsibilities to students, faculty, staff, and the constituents whom it serves. Federal and State statutes, rules, and regulations, State OIT Policies and standards, Louisiana Board of Regents policies, Louisiana Community and Technical Colleges System (LCTCS) policies and other explicit agreements also mandate the security of information and information systems. Failure to protect the College's information technology assets could have financial, legal, and ethical ramifications.

1.1 Policy Purpose

In fulfilling this mission, the College is committed to providing a secure yet open network that protects the integrity and confidentiality of information resources while maintaining its accessibility.

This document constitutes a College-wide security policy to address security issues related to the safety and integrity of information maintained on Delgado's computerized information systems through technology resources. This policy is not intended to address the proprietary interests of intellectual property and/or copyright issues. It is not intended to be an exhaustive document, but a guide which outlines the College's expectations and user responsibilities to follow; it is a living document.

1.2 Management's View and Enforcement of Security

The College acknowledges that no individual is immune from investigation when there is reasonable suspicion of theft, fraud, or misuse of Delgado's information technology resources.

In accordance with the [Louisiana Community and Technical College System Use of Technology Resources Policy Statement](#), use of Delgado Community College computer resources is limited to Delgado faculty, staff, currently enrolled students, and authorized guests, for legitimate academic and business purposes consistent with the College's mission. Use of technology resources of this institution is a privilege and not a right. Abuse of these privileges may result in the loss of such privileges, possible employment termination, student expulsion, and/or prosecution.

The unauthorized use of another's logon id and password will be viewed as theft of a College resource and computer fraud. The result of such abuse may be the loss of all computer privileges and/or other disciplinary action.

1.3 Security Policy Objectives and Methods

This policy attempts to outline security practices and how the College intends to manage, protect and distribute its sensitive information and the framework for securing its technology resources.

As a means of securing its technology resources, the College utilizes one or more of the following measures:

Authentication

- Traditionally, a *logon id* and *password* is used as assurance or verification that the resource (human or machine) at the other end of the session really is what it claims to be before being granted access to College resources. Authenticated users may have different types of permissions based on their authorization levels. As a means of authentication and control, a user may be required to provide proof of identification before being granted access to any College computer resource.

Authorization

- Most computer security systems are based on a two-step process with the first stage being authentication and the second stage being authorization. The authorization process allows a user access to various resources based on identity. It protects against unauthorized access to a system or to the information it contains by the types of permissions granted – **Access Control**.

Confidentiality

- Recognizing that confidentiality is critical to total data security, a number of tools are used to safeguard the confidentiality of Delgado's information, integrity, and non-repudiation of data (proof to receiver that sender is the originator of the information) and to assure that sensitive information remains private and is not visible to an eavesdropper. This includes but is not limited to:
 - **Encryption** ensures that classified information is not adversely affected;
 - **Virus Control** helps protect against file corruption;
 - **Electronic Data Exchange** by use of secure protocols, digital certificates and the Secure Socket Layer (SSL) to help ensure confidentiality and integrity when transmitting data across the network.

Audit

- Security-relevant events are monitored to provide logs of access attempt.
- Audit service tools will be provided to audit personnel to generate reports to analyze and review information technology security.

Administration

- The management of technology resources protection scheme ensures that only authorized users can access objects on the system. This is handled by creation, maintenance, and monitoring security information such as access control policies, authorized user profiles, security parameters, and ownership identification.

Network Security

- Firewall technology is used as protection of data against unauthorized access from untrusted network environments. In addition to firewall technology, intrusion detection software is used to ensure protection.

2.0 Security Personnel

2.1 Chief Information Security Officer

While Chief Information Security Officer is not an official title at Delgado, the Assistant Vice Chancellor/Chief Information Officer primarily assumes this role. The Assistant Vice Chancellor/Chief Information Officer is responsible for the security of the College's communications and technology resources, including the planning for and managing of an information technology disaster recovery plan. This individual is involved in both the business (including people) and technical aspects of security.

2.2 Internal Controls Administrator

This individual serves as lead security analyst in the Office of Information Technology and is a direct report to the Assistant Vice Chancellor/Chief Information Officer.

- Manages the information security function in accordance with established policies, guidelines, controls, and compliances.
- Provides direction and recommendations for the creation of a College-wide security policy and disaster recovery plan.
- Oversees account creation and maintenance procedures.
- Coordinates information security efforts as directed by the Assistant Vice Chancellor/Chief Information Officer.
- Analyzes security incidents and escalation of security events.
- Provides periodic reporting on information security issues.
- Supervises the Security Analyst.

2.3 Security Analyst

This individual is a direct report to the Internal Controls Administrator.

- Responsible for account creations for most technology resources.
- Assists with the development and maintenance of security policies and procedures.
- Provides recommendations and maintenance for the College-wide security policy and disaster recovery plan.
- Makes recommendations to Internal Controls Administrator regarding security operations.
- Alerts Internal Controls Administrator of possible security violations.
- Assists with other security related events and projects.

2.4 Network & Communication Services Manager

As the College's dependence on the network for daily business continues to increase and the services being used are becoming increasingly performance-sensitive, the importance of maintaining a centrally designed and managed network infrastructure becomes increasingly necessary. This individual is a direct report to the Assistant Vice Chancellor/Chief Information Officer and oversees the overall network security.

- Establishes and maintains hardware and software to promote uninterrupted operation of network-based application systems and to lessen exposure to accidental or intentional destruction, disclosure, modification, or interruption of information via the College's network.
- Serves as an internal consultant on network security issues.
- Uses various utilities to monitor network traffic and to detect possible intrusion.

3.0 Electronic Mail (E-mail)

3.1 E-mail Purpose

Delgado Community College employees and students have access to electronic mail (E-Mail) both internally and through the Internet. This E-mail access is the property of the College and may be subject to auditing and monitoring.

- Use of Delgado's E-mail system provides communication between staff, faculty, students, external entities, clients, and others.
- It is intended for business and academic use only.

3.2 E-mail Privacy

Users should not have any expectation of privacy when using and storing information on any computer resource of the College.

- The College reserves the right to review and copy any data or other information stored on any computer resource without notice to the user. E-mail created or distributed through Delgado's E-mail system is the property of Delgado Community College.
- Users should be aware that under certain circumstances, the Office of Information Technology staff may need to access and review E-mails sent and received.
- Users should remember that all E-mail sent or received through this system is the property of Delgado Community College, and is subject to audit and monitoring.
- There is no guarantee of security or confidentiality for inappropriate use of the E-mail system.

3.3 E-mail Usage

- E-mail should be transmitted based on business or academic need.
- Under no circumstance is it permissible for Delgado employees to conduct business of any kind that would infringe on the beliefs of the College.
- Users should not use E-mail to transmit messages that contain remarks, images, or content that can be considered defamatory, offensive, harassing, disruptive, derogatory, racial or ethnic slurs or as pornographic comments or images.
- It is strongly recommended that E-mail is not used to transmit passwords or any other authentication information for Delgado's systems.
- It is strongly recommended that confidential information is not sent in detail via the E-mail system when communicating with the Human Resource office (i.e., Password, SSN, DOB, Pin, etc.)
- It is prohibited that student grades or any sensitive material be transmitted in violation of FERPA guidelines.
- Users should never E-mail or otherwise transmit any attachment that is suspect of being a virus.

- Inappropriate use of the E-mail system **may** result in immediate loss of E-mail privileges and possible disciplinary action up to and including termination.

Examples of inappropriate usage include, but are not limited to, sending electronic chain mail or mass unsolicited mail, and altering email or Internet headers to hide the identity of the sender/poster or to attribute the email or posting to someone other than the sender/poster or intended recipient.

- Only responsible administrators or their designees are authorized to send broadcast e-mail communications to all faculty and staff. These general office email accounts have been set up to allow certain academic and administrative departments to disseminate highly targeted communications throughout the Delgado community. All Delgado responsible administrators and designees will retain their individual e-mail accounts.
- The Responsible Administrator for each area must sign a *Faculty/Staff Email Account Authorized User Agreement* form that states his/her responsibility. The user agreement authorization form is kept on file in the Responsible Administrator's office and the Office of Information Technology.
- Blackboard Community users are expected to adhere to the same policies regarding sending broadcast email communications to all faculty and staff.
- Only specifically identified email accounts are authorized to send broadcast email communications to students.
- Email accounts are provided to adjunct faculty when requested by the division for the time period as specified on the request.
- Only individuals authorized by their respective divisions are allowed to retrieve and distribute access letters to adjunct faculty.
- Employees with emeritus standing are allowed to retain their Delgado email account upon retirement.

4.0 Internet Usage

Delgado Community College provides Internet access for its employees so they can obtain up-to-date information that may be useful in performing their job responsibilities and duties.

4.1 Proper Internet Usage

- No illegal or pirated information or software should be downloaded or viewed.
- Passwords for personal use should be of different variation from those used within Delgado.
- Delgado prohibits employees from using the Internet to visit sites that are pornographic, sexually explicit, racial or ethnically biased or harassing or offensive in any way, either graphic or in text form, other than authorized academic purposes.
- Delgado reserves the right to monitor any and all network activities to and from your computer including Internet access. Such activities may be archived and monitored at a future date.

- Similarly, the unauthorized copying of commercial software packages for which the College is liable through licensing agreements or the introduction of any unauthorized software to a College computer is considered inappropriate and a violation of Internet usage and/or copyright laws and may be prosecuted.
- The Delgado Community College Home Page on the Internet is an official publication of the College. All web pages linked to it are also official publications of the College. These pages represent the College electronically, just as the *Delgado Community College Catalog* and the *Class Schedule* do in the print medium. As such, the content of these pages should promote the College, its programs, faculty and staff in a positive light, consistent with its mission.
 - The creation and maintenance of web pages by units within the College are encouraged as a means of promoting Delgado Community College, its programs, faculty, and staff.
 - These pages require the approval of the office of Public Relations and Marketing before publication and must be administered according to the College's [Internet Web Pages](#) policy.
- Inappropriate Internet usage will result in the loss of Internet access and may result in further disciplinary action, up to and including termination.

4.2 Wireless Access

Wi-Fi Purpose

Delgado Community College (Delgado) is the host to a Wi-Fi network that is available to employees, students, and authorized guests.

- Employees and students use their Delgado email account username to connect to the Wi-Fi network.
- Upon request, a special user account can be set up for doing business with the college for a specified time period.

Wi-Fi Usage

- Wi-Fi coverage is campus-wide at all Delgado locations.
- Access is available to connect to the Internet via devices such as laptops and mobile phones.
- Individual users must configure personal devices for wireless network connection.
- Department heads must request access for temporary use via the OIT Help Desk online system.

5.0 Software

Standard software applications have been loaded on each administrative employee's computer consistent with the needs of his or her position. Any modifications to this installation need the approval of the User Support Services Manager. OIT User Support Services will not support unapproved software.

5.1 Downloading and Installing Software

- Only licensed software compatible with Delgado's information systems will be installed on all Delgado technology resources.
- The staff of the Office of Information Technology (OIT) department will install the software according to the Office of Information Technology department guidelines for administrative PCs.
- Authorized lab assistants in the respective academic areas will install software according to the Office of Information Technology guidelines for faculty and student computing resources. OIT will provide technical assistance in those academic areas without a lab assistant.

6.0 End-User Account Access

The College is linked to the Internet and to other networks either directly or indirectly. Access to these networks by faculty, staff, and students is granted because of employment or enrollment at the College.

Delgado faculty and staff members may be granted access to the College's network and mainframe if deemed appropriate for their position or department. For detailed instructions on how to become a user of the College's network and/or mainframe systems, employees should refer to the College's [Technology Services](#) policy.

Since user account access is an integral part of security for the College's technology infrastructure, access is granted based on a number of general practices. The following guidelines have been established.

6.1 Account Creation

A request for account access is submitted electronically via the OIT Help Desk system. When a request is submitted, it is electronically routed for approval to the employee's supervisor and data manager, if applicable.

- The employee's job function and department requirements will determine the level of access to system resources.
- At a very minimum, all accounts require both a username and a password.
- Sharing of end-user accounts between users is prohibited.
- When an account has been established, electronic notification will be sent to the requestor and the new employee's supervisor.

6.2 Account Logons and Passwords

Delgado faculty, staff and students may be issued logon ids that are used to access various information technology systems and resources provided by the College. This logon id will remain valid for the period the individual is associated with the College.

All users with logon ids and passwords to the College's technology resources should be aware of the following:

- The logon id owner is responsible for all actions and functions performed by his/her logon id.

- Passwords used in association with the logon ids are to be safeguarded and neither logon ids nor passwords are to be shared by any two individuals. (*with the exception of general office email accounts and lab account*)
- Logon ids or passwords **may not be shared** with another person other than a designated OIT representative.
- End-users are limited to five (5) incorrect sign-on attempts before the logon id/account is automatically locked.
- Proper use of the logon id is the responsibility of the individual under whose name it has been assigned.

6.3 Password Selection and Management

Potentially, serious damage can occur if a user's password is not safeguarded. Therefore, passwords should be changed regularly. Passwords are used to authenticate an end-user's identity and to establish accountability. A password that is easily guessed is not an effective password and compromises security and accountability of actions taken by the logon id, which represents the end-user's identity.

All end-users with logon ids and passwords to the College's technology resources should practice the following:

- The recycle or re-use of passwords shall be reasonably limited.
- Users are advised to change the initial password on a new account immediately.
- Passwords should be selected that are difficult to guess by others.
- Mainframe passwords should be at least four (4) characters in length, must be in lower case, and may consist of a combination of letters, characters, and numbers (alphanumeric).
- Network passwords should be at least twelve (12) characters in length.
- Network password complexity must contain at least 3 of the following 4 categories: English upper case characters (A-Z), English lower case characters (a-z), Base 10 digits (0-9), and non-alphanumeric characters (e.g. %, &, !).
- It is strongly suggested that passwords should not include your logon id, your name, your spouse's name, children's or pet's name, or any other names commonly known to others.
- Users will be held accountable for password selection and protection.
- A user's password must not include anything derogatory, offensive, or defamatory.
- It is strongly suggested that passwords are not written down or stored in a place that can be accessed easily by others.
- All passwords shall be changed whenever it is determined that a system security may have been compromised.
- When requesting a password reset, individuals will be asked a security question(s) to verify the identity of the person requesting the action.

- After five (5) unsuccessful attempts are made to enter a password, the logon id will be automatically locked. When this occurs during regular business hours (8am – 4:30pm – CST), the authorized user may call the OIT Help Desk for assistance. When this occurs after regular business hours (4:31pm – 7:59am – CST), the authorized user may call the 24/7 Support Center for Delgado Community College at 1-866-271-1458 or visit the Online Support Center at <http://d2.parature.com/ics/support/default.asp?deptID=8095>.
- Passwords are encrypted and will not display when typed.
- Mainframe passwords should periodically be changed. However, it will automatically expire every 180 days; the system will prompt you when the time approaches. **Note:** The 180th day for each individual may be different.
- Network passwords should periodically be changed. However, it will automatically expire every 105 days; the system will prompt you when the time approaches. **Note:** The 105th day for each individual may be different.

Some general management rules to practice are: 1) do not leave your computer logged on and unattended for an extended period of time, 2) do not log on to your system if someone can see you keying in your password, 3) turn off your computer when you leave for the day, 4) if you use a remote access program and you need to leave your computer on, be sure that it is in a locked room, and 5) use a screen-saver access program to secure the computer from unauthorized access.

6.4 Temporary or Contracted Employees

All temporary and contractual employees with access to the network or mainframe should be aware of the following:

- Accounts are created for Temporary or Contracted employees using the same process as regular employees.
- All Temporary or Contracted employees must be set up with a temporary account containing an account expiration date, if applicable.
- Upon approval, the Office of Information Technology will provide a logon id and password for temporary access and application use.

6.5 Account Modification

Current employees may request changes to their access by submitting the appropriate access request update form through the online OIT Help Desk system. The employee's supervisor must approve the request electronically. However, this does not automatically guarantee that the request will be granted, as it may require the approval of a data manager, if applicable.

6.6 Account Removal

All employees with access to the network or mainframe should adhere to the following:

- When OIT is notified of an employee's separation from the College, access to technology resources will be disabled. Access is not removed until confirmation of separation is received from the Human Resources office.
- Access to technology resources will be restricted by the close-of-business on the employee's last working day, unless otherwise instructed by Human Resources.

- In the event of immediate access suspension, an authorizing College administrator contacts the Office of Information Technology Assistant Vice Chancellor/CIO or the Internal Controls Administrator. The Assistant Vice Chancellor/CIO or Internal Controls Administrator notifies the appropriate security personnel so that the access to technology resources is immediately disabled.
- Retirees will not retain access to their email account upon separation from the college.
- Student email accounts are purged annually. Student email accounts are purged from the email database based on criteria provided by the College Registrar.

6.7 Remote Access

Delgado Community College adheres to the Louisiana Community and Technical College System's policy regarding remote access.

- Remote access users shall not violate any college policies, perform any illegal activities, and be used for outside business interests.
- Remote access privileges will be strictly limited and evaluated on a case by case basis.

7.0 Physical Controls

Central access controls are assigned to the College's Campus Police Department. Acting as the Central Access Control Administrator, the Campus Police Department under the direction of the Chief of Police is responsible for the utility, security, maintenance and coordination of the card access system and managing access to facilities as stated in the College's [Access Control Procedures](#) policy.

- The Campus Police Department provides authorized employees with access to buildings and offices when metal keys or access cards are not available and conducts daily physical security inspections of facilities.
- The issuance of keys to all college facilities is managed by Campus Police Department.

7.1 O.I.T. Area - Physical Controls

Access to the area where the Office of Information Technology is housed is controlled by card access restricted to authorized personnel. During regular business hours, access to the lobby area through the front entrance door is unrestricted. Access to all other areas (staff office area, data center) is restricted and requires authorized access cards or metal keys for entry.

- Access is restricted by class (days, time periods and type), which determines access entry to the general office area and the data center.
- Authorized visitors are supervised and their entry and exit is recorded in a log.

7.2 Computer Theft

As computer theft is and will continue to be a problem, individual users are responsible for securing their PCs and laptops. Stolen hardware will immediately be reported to Campus Police. If that theft results in the loss or compromise of sensitive information, the type and nature of the data lost will also be reported to the Security Unit of the Office of Information Technology. If the computer was acquired from OIT, a copy of the Campus Police Report must be forwarded to OIT for its records.

7.3 Locks

Physical security is a key to protecting computers and computer information from loss and damage. All media and other sensitive information must be stored in a secured area. It is expected that computers be turned off when not in use for an extended period of time and office doors locked as applicable. It takes only a few minutes to practice good physical security.

7.4 Portable Devices

Off-campus users must take additional precautions to safeguard computer information and equipment, including but not limited to:

- Safeguarding the computer and information from theft or damage.
- Prohibiting access to the computer (including family, friends, associates, and others) for any purpose, without departmental authorization.
- Ensuring all sensitive data on approved portable storage devices is properly encrypted (see 15.3 Data Security- Encryption);
- Adhering to all computer policies and practices of the College, LCTCS and the State of Louisiana.

8.0 Security and Responsibilities

All users have the responsibility to operate the College computing systems in an ethical, lawful, and responsible manner. These principles of responsible use are derived directly from standards of decency and common sense that apply to the use of any shared public resource. They apply equally to users who are students, faculty, staff, or any authorized guest user of the College's systems, networks, and services.

Delgado Community College will hold responsible the owner of any account through which security violations or irresponsible use occurs. Delgado Community College also reserves the right to withhold computing privileges from those who do not abide by the letter or intent of this policy document. Violations of this policy by students shall be treated as violations of the [Student Judicial Code](#) and will be referred to the Office of the Vice Chancellor for Learning and Student Development for handling. Faculty and staff members who violate this policy will be subject to College disciplinary action.

These responsibilities are delegated to the following group of individuals:

Administrators must:

- be responsible for maintaining the integrity of computer systems and data held on them, and for ensuring the systems are not misused;
- identify the electronic information resources within areas under their control;
- define the purpose and function of the resources and ensure that requisite education and documentation are provided to the College as needed;
- establish acceptable levels of security risk for resources by assessing factors such as:
 - how sensitive the data is, such as research data or information protected by law or policy,
 - the level of criticality or overall importance to the continuing operation of the campus as a whole, individual departments, research projects, or other essential activities,

- how negatively the operations of one or more units would be affected by unavailability or reduced availability of the resources,
 - how likely it is that a resource could be used as a platform for inappropriate acts towards other entities,
 - limits of available technology, programmatic needs, cost, and staff support;
- ensure that requisite security measures are implemented for the resources;

Data Managers are:

- responsible for determining how the data may be used within the various applications, existing policies, and authorizing who may access the data;
- responsible for authorizing user access relevant to the specific system under their management;
- responsible for determining the type of access granted to each specific user.

End-User will:

- adhere to the highest standards of ethical, responsible and considerate uses of technology resources, and avoid those uses prohibited by law or other directives;
- **not** disclose information in the data nor the access controls over the data unless specifically authorized in writing by the data manager;
- use data only for purposes specified by the data manager;
- ensure all sensitive data on approved portable storage devices is properly encrypted (see 15.3 *Data Security- Encryption*);
- comply with security measures specified by the data manager;
- **not** modify or reconfigure any component of computing resources without proper Office of Information Technology authorization;
- **not** attempt to gain access to any computing network, academic or business resources that the end-user is not authorized to use, in other words "hacking";
- **not** connect or install any unauthorized hardware or equipment including, but not limited to, laptops, external drives, etc., to any technology resources or network access points without prior written approval from the Office of Information Technology;
- be considerate in the use of shared technology resources, coordinating with the Office of Information Technology for "heavy use" operations that may unduly slow operations for other users;
- comply with Computer Learning Laboratory guidelines and rules as set forth by the College's [Computer Learning Laboratories](#) policy and appropriate campus official(s);
- accept full responsibility for any publication resulting from technology resources and/or publishing web pages and similar resources, including ensuring that all copyrights have been authorized for use;
- **not** accept payments, discounts, free merchandise or services in exchange for any services provided through use of the technology resources, unless properly authorized by the College, or otherwise conduct a for-profit, commercial business without properly coordinating with authorized Delgado administrators;

- **not** participate in gambling and peer-to-peer sharing on the Internet unless specifically authorized and/or provided by the College;
- **not** create or connect a server to the network without written permission from the Office of Information Technology;
- **not** play games on the network or shared computing resources for non-academic purposes;
- **not** use talk, write or IRC (inter-relay-chat) resources for non-academic purposes or in an abusive or frivolous manner;
- **not** post non-academic and/or inappropriate material to the Internet or a Website;
- **not** use large amounts of disc space to store files not related to the individual's institutional duties or for which an individual does not have proper permission to store or distribute (for example, using file sharing services such as Kazaa, Napster, Morpheus, etc.);
- **not** execute programs that have no useful purpose, thus taxing the system's resources;
- **not** use the computing network, academic or business resources of Delgado Community College for activities that are illegal (for example, child pornography, etc.).

OIT Staff will:

- **not** be permitted to provide access to data without authorization from the appropriate data manager;
- be provided with privileged access to computer systems in order to carry out their responsibilities. They have a duty to use such privilege at all times in a professional manner and within the interest of the College;
- be responsible for email services that connect either to the Internet or public telephony services and make all reasonable efforts to inform their users that traffic may be recorded or monitored in compliance with the Regulation of Investigatory Powers Act (2000);
- become knowledgeable regarding relevant security requirements and guidelines;
- analyze potential threats and the feasibility of various security measures in order to provide recommendations to administrative officials;
- implement security measures that mitigate threats, consistent with the level of acceptable risk established by administrative officials;
- establish procedures to ensure that privileged accounts are kept to a minimum and that privileged users comply with privileged access agreements;
- protect individual passwords;
- **not** browse, inspect or copy users' information;
- **not** routinely collect information on individuals' information usage patterns;
- **not** configure software systems so as to maximize the confidentiality of user communication;
- configure systems to enforce appropriate password policies;
- stay abreast of any vulnerabilities of systems and manage security in accord with appropriate recommendations;
- configure systems to minimize the chance for abuse, and act promptly to end abuses upon notification.

9.0 Virus Detection Software

Virus detection software is primarily used for the prevention of virus outbreaks and attacks involving computer resources. Licensed virus software is used to ensure the integrity, reliability, and good performance of College computing resources. As such:

- Administrative desktop computers and network servers are required to have *Delgado* approved virus detection software.
- Administrative desktop computers must be configured to have the virus detection software scan periodically (at least monthly) for viruses.
- Administrative desktop computers must be configured to have the virus detection software download and update the virus definitions on a periodic basis (at least monthly).
- Authorized lab assistants in the respective academic areas will configure desktop computers with authorized virus detection software and standard desktop components for faculty and student computing resources. OIT will provide technical assistance in those academic areas without a lab assistant.

10.0 Social Engineering

The basic goals of social engineering are the same as hacking in general: to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network. Social engineering attacks typically take place on two levels: the physical and the psychological.

These engineering attacks are achieved through a number of tactics such as:

- ◆ **Social Engineering by Telephone**
A hacker will call up, imitate someone in a position of authority or relevance, and gradually pull information out of the user.
- ◆ **Waste Management**
Also known as “trashing” or “dumpster diving,” this involves searching trash for valuable information.
- ◆ **Online Social Engineering**
Through anonymity of the Internet, this tactic enables hackers to make approaches to users for valuable information.
- ◆ **Persuasion**
The main objective is to convince the person disclosing the information that the social engineer is in fact a person he/she can trust with that sensitive information.
- ◆ **Reverse Social Engineering**
This is when the hacker creates a persona that appears to be in a position of authority so that users will ask him/her for information, rather than the other way around.

A few helpful tips for deterring possible attacks of “social engineering”:

- Use caution when executing sensitive programs or entering logon information in the event of possible “shoulder surfing”.
- Use caution with sensitive documents and be sure to shred documents when discarding to prevent retrieval of valuable information.

- Lock workstations when away to avoid such activity of “password grabbing”.
- Use caution when asked to provide personal information via the Internet.

11.0 Privacy of Students

The Family Educational Rights and Privacy Act (FERPA) protect educational records of a student from public disclosure without written permission of the student. Delgado Community College adheres to these rules and guidelines to protect the rights of its student body. The College’s computing information and network resources are used in a manner that complies with this privacy.

12.0 Telecommunications

Overall, the Office of Telecommunications Management (OTM) is responsible for management of telecommunications within the executive branch of Louisiana state government. This includes the planning, procurement, provision, and administration of both goods and services statewide. The College’s Office of Information Technology (OIT) operates as the liaison between OTM and the College. The Telecommunications section of OIT is responsible for the wiring, cabling, maintenance, and leasing of services for the operation of the College’s communications.

Additionally, the Telecommunications section of OIT is responsible for wireless data transfers, voice communications, telecommunications equipment and requests for modifications to existing telecommunications equipment, systems or services, coordinating with OTM for the acquisition of new telecommunications systems or services and the like.

All telecommunications resources connected to or used through the College and any telecommunications services used on the College provided telephone network are to be controlled. Some of the technology resources provided by the College are as follows:

Voice Access and Service

Voice communications is another essential tool required for Delgado Community College to accomplish its mission. It, like data transmission, must be used correctly for it to produce significant efficiencies and improved productivity. The same standards of decorum, professionalism, and respect that guide us in our face-to-face interactions apply to the use of voice transmissions.

Voice Services

The College’s **telephone system** is currently owned by the College maintained by the Office of Information Technology.

- Telephone service is available to employees to conduct College business. Employees should not utilize the College’s telephone system for personal use. However, the College does realize that emergencies do arise where the telephone must be used for personal situations, i.e. family emergencies.
- Public telephones are located throughout the various College locations for the personal use of students, employees and others who may require telephone access.
- Department heads determine what telecommunications devices and services are required by the employees under their supervision and then submit a service requests via the OIT Helpdesk system.
- Requests for modification to telephone services must be submitted to the Office of Information Technology’s Telecommunication section via the OIT Help Desk system.
- Users are responsible for informing OIT in the event of transmission problems.

Voice Mail

- It is imperative that voice mail be checked on a daily basis, and messages appropriately acted upon.
- It is everyone's responsibility to help decrease and eliminate voice mail complaints.
- It is necessary that voice mail greetings and name be updated so that callers will not think they were given the wrong person or extension when calling.

Supplied Cellular Phones

Upon request, [cellular phones](#) will be provided to Administrators in the position of Dean or above; and employees designated by the Vice Chancellor for Business and Administrative Affairs, with approval by the Chancellor, whose positions provide a legitimate business need for cellular phone service.

Hand-Held Communication Devices

BLACKBERRY

Upon request, a [Blackberry](#) will be provided to Administrators in the position of Dean or above; and employees designated by the Vice Chancellor for Business and Administrative Affairs, with approval by the Chancellor, whose positions provide a legitimate business need for hand-held communication service.

TWO-WAY RADIOS

Upon request, [two-way radios](#) will be provided to employees designated by the Vice Chancellor for Business and Administrative Affairs whose positions provide a legitimate business need for two-way communication with other designated employees.

- Cellular phones will be purchased by the College and shall remain the property of Delgado.
- Cell phone usage should be limited to College-related business.
- Emergency Response Team members have been given alternate cellular services in the event of an emergency.
- Satellite phones have been issued to key administrators for use in cases of emergency events.

Termination of Employment

- When *an individual* separates from the College, he/she must return all communication devices during the exit process.

13.0 Confidentiality

All computer information is considered confidential unless a user has received permission to use it. Accessing or attempting to access confidential data is strictly prohibited. Confidential information should only be used for its intended purpose. Using confidential information for anything other than its intended use, without prior approval, is prohibited.

Delgado strives to maximize the confidentiality and security of its information systems and services within the limitations of available resources. As with paper-based systems, no technology can be guaranteed to be 100% secure. All users should be aware of this fact and should not have an expectation of total privacy regarding information that is created, stored, sent, or received on any networked system. The College reserves the right to review and copy any data or other information stored on any computer resource without notice to the user. This also includes the monitoring of all Internet use, email, and other activities accessed on or through computer resources of the College. Such monitoring, without limitation, may include, but is not limited to, review of all sites accessed by a user and e-mails transmitted and/or received.

The Internet environment offers tremendous opportunities to provide convenient access to information and services to authorized individuals wherever they may be. Users who serve as data managers of institutional information should be particularly aware of the potential for unauthorized access to or tampering with online information and services in the Internet environment.

The Office of Information Technology (OIT) is responsible to provide reasonable measures of protection for confidentiality via technology resources. Windows authentication and encryption as well as SSL (Secure Sockets Layer) secure encryption is currently used to safeguard personal information transmitted over the Internet. In addition, information is scrambled to enhance security when transmitting sensitive information.

14.0 Data Sanitization

Information is the engine of an organization and is undoubtedly a powerful asset but it can also threaten an organization's existence if it falls into the wrong hands. In this advanced technological age, virtually every educational institution is fully reliant on information technology assets in their day-to-day operations. Large volumes of confidential data such as student records, financial assistance information, financial records, and personnel data are stored on PCs, posing a significant security threat. A single improperly discarded hard drive or PC could have severe consequences if proper measures are not taken to prevent the unauthorized disclosure of confidential data.

Delgado Community College complies with the State of Louisiana Office of Statewide Technology Policy #IT-POL-003, *Data Sanitization (Transfer and Disposal of Personal Computer Equipment)*, and the software licensing agreements under which software is obtained.

In accordance with these regulations, Delgado has implemented its [Transfer and Disposal of Data Storage Devices](#) policy, whereby the College determines and uses an appropriate method to sanitize magnetic storage devices, optical storage media and non-volatile memory devices that are surplus, transferred to another government entity, or subject to destruction. These methods include overwriting all addressable data locations on the device and/or mechanically magnetizing (e.g., degaussing) the device.

Sanitization is the secure removal of data and software from IT equipment before disposal. Generally, the Office of Information Technology will sanitize operable computers by the execution of a program that overwrites all data and programs on the hard drive.

15.0 Data Security

Data of value (data that would be missed if lost and cannot be easily recreated as from an OS installation) must be backed up on a regular basis. The Office of Information Technology must ensure that a means of backing up and restoring vital data is provided; in keeping with this responsibility, a backup strategy for the College's network and mainframe systems is conducted on a daily basis.

15.1 Data Security – Backups

Networking

The entire backup process is hosted by our Disaster Recovery site, VENYU. VENYU *DataVault* Agents are installed on each server/workstation requiring backup. Each agent is configured to transmit and store the backed-up data at the secure data vault located at the VENYU data center(s). VENYU ensures that the data is always encrypted throughout the backup, data transfer and retrieval processes and its *DataVault* technology provides a secure solution to protect critical data.

The backup process is completely automated requiring minimal intervention from the Network Analyst. The backup process consists of two strategies, which are the "incremental" and "full" backup strategy. The incremental backup runs daily and full backup runs on Saturday evenings.

Mainframe

Daily backups of the College's mainframe computing system are performed to ensure availability and integrity of data. The backup process consists of basically two strategies, "incremental" and "full" backups.

- Each day incremental backups are taken of all DASD datasets to which modifications have been made since the last backup taken.
- Periodically, full volume backups are made of each disk pack. These full volume backups occur automatically as a new generation of backups.
- In addition to the generation that is currently being built, four complete generations are available from which restorations may be done.
- Two copies of each backup/archive are made. One copy is vaulted offsite for disaster recovery purposes and the other copy remains onsite for system restoration, if needed.
- A Tape Management System (TMS) vaulting procedure is used to automate the vaulting rotations.

15.2 Data Security – Auditing and Monitoring

The Office of Information Technology is responsible for the monitoring and periodic audits of the College's technology resources including, but not limited to, technology systems, software development, and operating systems. To facilitate this effort, a number of tools are used, such as:

Audit Logs – logs are maintained that can provide sufficient data to reconstruct events and actions, such as dates, times, individual and/or process authorizing an activity/operation.

Archives – information is archived to ensure that important assets are maintained in a reliable long-term retrieval state for specified periods that may be utilized for special needs (i.e. – legislation, statutes, government, etc.).

Monitoring Products – a number of monitoring utilities are used to monitor the College's network infrastructure. These tools allow for the monitoring of Internet connectivity, servers, routers, switches, ports and the like.

Audit Files – are available through the College's administrative applications that allow for audit tracking of data elements in the databases. Reports can be generated indicating the before and after values of the data element. Event logs on the network automatically record network activity and 'flag' possible suspicious activity or concerns.

System Review – security reports are generated periodically for review by the specific data manager of each system (FRS, HRS, SIS) to maintain access control to the College's administrative applications. These reports also provide a mechanism to assist with maintaining access control for network user accounts.

15.3 Data Security – Encryption

As stated in the State of Louisiana OIT Policy #IT-POL-014, sensitive data, defined as data not subject to the Louisiana Public Records Act (L.R.S. 44:1 et seq), is to be encrypted on all approved portable storage devices. The state's preferred encryption freeware is "TrueCrypt," which is available to download and view tutorials at <http://www.truecrypt.org>.

15.4 Data Security – Retention and Compliance

It is recommended that data/files are maintained for a period of five (5) academic/calendar years.

16.0 Reporting Violation Incidents

16.1 Technology Security Violations

Reporting incidents is an ethical responsibility of all members of the Delgado Community College community. A critical component of security is to address security breaches promptly and with the appropriate level of action. Below are guidelines for reporting and handling security incidents:

- All users of Delgado Community College technology resources computers have the affirmative obligation to report, directly and without undue delay, any and all information concerning conduct that they know to involve corrupt or other criminal activity or conflict of interest to the College.
- Activities that should immediately be reported include, but are not limited to:
 - Attempts to circumvent established computer security systems;
 - Use, or suspected use, of virus, Trojan Horse, or hacker programs;
 - Obtaining, or trying to obtain, another user's password;
 - Using the computer to create and/or disseminate harassing or defamatory messages;
 - Using the computer to communicate inappropriate messages or jokes that may be considered offensive by others;
 - Illegal activities of any kind;
 - Attempts to breach facility security should be reported to Campus Police;

Incidents of security violations, willful or intentional, of secured resources are considered to be misconduct under applicable student and employee conduct standards. Users engaged in such conduct may be denied access to technology resources and may be subject to other penalties and disciplinary actions including termination or expulsion.

Under appropriate circumstances, Delgado Community College may refer suspected security incidents to law enforcement authorities, and provide access to necessary data for investigation as permitted by law.

Technology security violations can be reported in three ways:

- 1) Send email to oitsecurity@dcc.edu
- 2) Visit Delgado Help Desk and complete the "Security Violation Incident Form"
- 3) Call OIT Help Desk

17.0 O. I.T. Internal Process for Acquiring Services

17.1 Network and Mainframe Access

Faculty and staff members may be granted access to the College's network and the College's mainframe if deemed appropriate for their positions or departments. To become a user of the College's computer system (network) and, if also deemed appropriate, the College's mainframe, an Access Request New User Computer Account Form must be completed and submitted electronically via the OIT Help Desk online system to the Office of Information Technology for processing. The Access Request New User Computer Account Form is also used to submit a request for a Delgado email account.

The three major applications accessed through the College's mainframe system are: (1) the Student Information System (SIS); (2) the Financial Records System (FRS); and (3) the Human Resources System (HRS). Each system, and the specific functions of the system, is overseen by data managers who are responsible for managing user access and security of specific function of the systems.

Requests for access to mainframe data or functions are to be made on the appropriate system access form, with the approval of the employee's supervisor and the data manager of the system. Access to the network and mainframe must be granted before an employee is granted access to the individual systems. Requests to update access are to be made on the appropriate system access update form. The following forms are required for obtaining and updating access on each system.

Student Information System (SIS)

To request access to the Student Information System, an Access Request New User SIS Form must be submitted electronically via the OIT Help Desk online system to the Office of Information Technology for processing. To update existing SIS account/access, an Access Request Update User SIS Account/Access Form must be submitted electronically via the OIT Help Desk online system to the Office of Information Technology for processing.

Financial Records System (FRS)

To request access to the Financial Records System, an Access Request New User FRS Form must be submitted electronically via the OIT Help Desk online system to the Office of Information Technology for processing. To update existing FRS account/access, an Access Request Update User FRS Account/Access Form must be submitted electronically via the OIT Help Desk online system to the Office of Information Technology for processing.

Human Resources System (HRS)

Because of the confidential nature of employee information, access to the College's Human Resources System is extremely limited. To request access to the Human Resources System, an Access Request New User HRS Form must be submitted electronically via the OIT Help Desk online system to the Office of Information Technology for processing. To update existing HRS account/access, an Access Request Update User HRS Account/Access Form must be submitted electronically via the OIT Help Desk online system to the Office of Information Technology for processing.

18.0 Policy Development, Approval, and Implementation

Development of this policy was primarily the responsibility of the *Assistant Vice Chancellor/ Chief Information Officer* of the Office of Information Technology and staff. To assist in facilitating this process, the ISC Security Policy Sub-Committee and a small group of selected Reviewers were solicited for additional contributions.

Approval of this Security policy is vested with the Administration who will rely on the recommendations of the Information Systems Council (ISC) and the College Council.

The *Assistant Vice Chancellor/ Chief Information Officer* of the Office of Information Technology has overall responsibility for the security of the College's information technology resources. Implementation of security policies is delegated throughout the College to various College services; to departments, and other units; and to individual users of campus IT resources.

19.0 Acknowledgments

Many people have contributed to this document, directly or indirectly. Delgado Community College gratefully acknowledges the assistance of the Reviewers, ISC Security Policy Sub-Committee, Information Systems Council (ISC), and the College Council.

In the spirit of acknowledgment, Delgado Community College wishes to thank the Louisiana Community and Technical Colleges System (LCTCS) for allowing the adaptation of material from its IT Security Policy.

20.0 Cancellation

This cancels "Information Technology Security Policy," dated May 7, 2010.

Glossary of Terms

FRS	Financial Records System
HRS	Human Resources System
OIT	Office of Information Technology
SIS	Student Information System
Access Control	Determines whether a user or entity is authorized to use a system, network, or resource.
Audit	An examination of records or financial accounts to check their accuracy.
Authentication	Protecting against unauthorized access to a system or to the information it contains by verifying the identification of a user or entity.
College	The institution of Delgado Community College
Confidentiality	The state of being secret; containing information, the unauthorized disclosure of which poses a threat to security.
Data Manager	A representative of the department responsible for maintaining current and accurate data elements in the automated files. Also referred to as, Custodian or Data Owner. (For example, the Registrar is the Data Manager for student records maintained on the Student Information System.) (See table below for Administrative System Data Managers).
Encryption	The activity of converting from plain text into code
End-User	The person who uses a computer application, as opposed to those who developed or support it. The end-user may or may not know anything about computers, how they work, or what to do if something goes wrong. End-users do not usually have administrative responsibilities or privileges.
Network Security	Preventing unauthorized access from <i>un-trusted</i> network environment through the use of firewall technology.
Password Grabbing	Using a program or procedure that looks like a normal logon process but instead records the user's password and user name.
Pirated	One who makes use of or reproduces the work of another without authorization.
Portable Storage Device	A device for recording (storing) information (data). A storage device may hold information, process information or both. <i>Examples:</i> Notebook PCs, USB Thumb Drives, USB Hard Drives, CDs, DVDs, PDAs, etc.
Responsible Administrator	The account manager who has the ability to designate an individual(s) to administer, manage and/or send out college-wide communications under the Faculty/Staff Email Account for the respective area. (See table below for authorized accounts)

Glossary of Terms (continued)

Security	In the information technology industry, refers to techniques for ensuring that data stored in computer resources cannot be read or compromised by an individual without authorization; precautions taken to guard against crime, attack, sabotage, espionage, etc.
Sensitive Data	Data not subject to the Louisiana Public Records Act (L.R.S. 44:1 et seq).
Shared Workstation Accounts	An account shared by multiple individuals to access a shared computer in an office or lab setting.
VPN	A VPN (virtual private network) is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network
Waste Management	(Dumpster Diving) Retrieving documents discarded in wastebasket or recycle bin, or copying documents left in unlocked drawers.
Wi-Fi	Wi-Fi (wireless fidelity) is a means by which portable devices can connect to the Internet wirelessly. A user account is required.

Delgado Community College Administrative Systems Data Managers		
Application	Subsystem	Data Manager
SunGard SIS Plus	Student Records	College Registrar
SunGard SIS Plus	Admissions	College Director, Admissions & Enrollment Services
SunGard SIS Plus	Financial Aid	College Director, Financial Assistance
SunGard SIS Plus	Bursar	Director, Accounts Receivable
SunGard FRS Plus	Financial Records	Assistant Operations Manager, Accounting
SunGard HRS Plus	Human Resources	Information Technology Applications Programmer /Analyst 2

FACULTY/STAFF EMAIL ACCOUNTS		
Displayed Name	User Name	Initial Responsible Administrator
Delgado Chancellor's Office	DCCCHAN	Larissa Littleton-Steib
Delgado Public Relations & Marketing Office	DCCPRM	Carol Gniady
Delgado Institutional Advancement Office	DCCIA	Nita Hutter
Delgado Learning & Student Development Office	DCCVCLSD	Debbie Lea
Delgado Faculty & Staff Professional Development Office	DCCFSPD	Cindy Siegrist
Delgado Distance Learning & Instructional Technology Office	DCCDLIT	Missy Lacour
Delgado Professional Development Academy	DCCPDA	Yvette Alexis
Delgado Student Affairs Office	DCCSA	Arnel Cosey
Delgado Business & Administrative Affairs Office	DCCVCBAA	A. C. Eagan
Delgado Controller's Office	DCCCO	Ronnie Rodriguez
Delgado Information Technology Office	DCCOIT	Thomas Lovince
Delgado Human Resources Office	DCCHR	Carmen Walters
Delgado Policy Office	DCCPOLICY	Karen Laiche
Delgado Campus Police Office	DCCCP	Ronald Doucette
Delgado Workforce Development & Education Office	DCCWFD	Kathleen Mix
Delgado Non-credit and Professional Development Office	DCCNCPD	Kathleen Mix
Delgado Classified Staff Organization	DCCCSO	Organization's President
Delgado Unclassified Staff Professional Organization	DCCUSPO	Organization's President
Delgado Faculty Senate	DCCFS	Faculty Senate President
Delgado Service Learning	DCCSL	Warren Punekey
Delgado Institutional Research	DCCIR	Cathy Sarrazin