TECHNICAL COLLEGE
TCSG
SYSTEM OF GEORGIA

Nathan Deal
Governor

Gretchen Corbin
Commissioner

August 11, 2015

President Ivan Allen
Central Georgia Technical College
3300 Macon Tech Drive
Macon, GA 31206

Dear President Allen:

Thank you for submitting the 2015-2016 Business Continuity Plan for your college. Your BCP has been approved without need for revisions. We appreciate the hard work and dedication you and your staff have shown.

If you have questions or need further information concerning applicable requirements, please contact me at (404) 679-1666 or lbeck@tcsg.edu.

Sincerely,

Lisa Anne Beck
Emergency Manager

(Please forward a copy to your College Business Continuity Plan Coordinator for college distribution.)

CENTRAL GEORGIA TECHNICAL COLLEGE

Business Continuity Plan

2015-2016

REVIEWED: _____ **DATE:** 4/15/15
CENTRAL GEORGIA TECHNICAL COLLEGE
BUSINESS CONTINUITY PLAN COORDINATOR

APPROVED: _____ **DATE:** 4-21-15
PRESIDENT/EXECUTIVE

REVIEWED: _____ **DATE:** 07/13/15
TECHNICAL COLLEGE SYSTEM OF GEORGIA
EMERGENCY MANAGER

APPROVED: _____ **DATE:** 8/7/15
TECHNICAL COLLEGE SYSTEM OF GEORGIA
ASSISTANT COMMISSIONER
DATA, PLANNING AND RESEARCH

CENTRAL GEORGIA TECHNICAL COLLEGE

2015-2016

CENTRAL GEORGIA TECHNICAL COLLEGE BUSINESS CONTINUITY PLAN

TECHNICAL COLLEGE TCSG SYSTEM OF GEORGIA

CENTRAL GEORGIA cgtc TECHNICAL COLLEGE

Table of Contents

I. GENERAL

Introduction

Business Continuity Planning is the process whereby organizations ensure the maintenance of critical operations when confronted with adverse events such as natural disasters, technology failures, human errors, or terrorism. The objectives of a business continuity plan are to minimize loss to the organization, continue to serve customers, and maintain administrative operations. The overall business continuity planning process is depicted in Figure 1.

Central Georgia Technical College has an obligation to protect and provide for students, faculty, staff, and visitors in the event of a major interruption of our mission or operation. These obligations extend to a responsibility for each Department to be able to meet its individual obligations. This includes the ability to provide the services expected of them and to carry out functions critical to the mission of Central Georgia Technical College should an event occur that interrupts the normal course of operations. Failure to have an adequate continuity plan could lead to financial disaster, interruptions of academic classes, and delays in completing other mission critical activities.

Scope

The Business Continuity Plan (BCP) is executed after health, life, and safety issues are addressed. As a minimum, the BCP assumes the following have been restored:

-Police, Fire, and Ambulance services
-Electricity, water, reasonable climate control, and adequate lighting
-Access to and egress from campus, classrooms, and administrative facilities
-Safe handling and proper disposal of toxic substances, biologically hazardous materials, and radioactive materials

The BCP shall contain clear strategies and procedures needed to continue operations and execute a recovery in the event of an interruption that compromises the ability of the operating unit to carry out its critical functions. The determination that an interruption has occurred may be made by the Technical College President or the Central Office. Business Continuity Planning encompasses maintaining and recovering the business, not just the recovery of technology.

Business Continuity Planning requires both a college-wide plan and individual plans for operating units that are responsible for mission critical functions. Mission critical functions are processes that are essential to ensure loss to the organization is minimized, constituents continue to be served, and administrative operations are resumed safely and effectively.

Authority

The State of Georgia continually establishes, maintains and directs activities related to Business Continuity and Disaster Recovery of all State Boards, Departments, Agencies, Associations, Institutions and Authorities. It is by Executive Order of the Governor of the State of Georgia that these plans be created, maintained, reviewed and updated for the purposes of preparedness for response to the effects of

emergencies and disasters and to protect public peace, health and safety and to preserve lives and property of the citizens of Georgia. The order was signed February 14, 2006.

Components

The commonly accepted components of a Business Continuity Plan are:

Business Impact Analysis – identifies critical business processes, assigns estimates of maximum allowable downtime, and designates priorities for restoration.

Risk Assessment – identifies specific threats, assesses vulnerability to those threats, and assigns degree of risk associated with each threat.

Risk Management/Continuity Planning – utilizes the Risk Assessment to determine which risks should be managed; and provides a written, widely disseminated, and exercised plan on actions necessary to get the business up and running in the event of disruption associated with those risks.

Testing and Updating – establishes mechanisms to exercise the plan and keep it current.

II. BUSINESS IMPACT ANALYSIS

The critical mission processes were determined and the interdependencies between those processes that must continue to exist for the Technical College to function. Critical processes generally fall into one of three general categories:

Safety and Security - Activities needed to sustain a safe and secure environment for students, faculty, staff, the visiting public, and surrounding community. While the Disaster Recovery Plan addresses restoring safety and security, the Business Continuity Plan may be concerned with sustaining those functions for an extended period.

Business Support Services - Activities that allow the Technical College to maintain necessary business operations, safeguard assets, and ensure the financial viability of the Technical College. Examples include payroll, revenue collection, accounts payable, and financial reporting.

Learning and Education - Activities that carry out or directly support the academic mission of the Technical College. For example, student support services (admissions, registration, etc.), lecture & study, graduation.

The Threat Assessment guides and identifies risks and/or hazards that might reasonably pose a threat to Central Georgia Technical College or an operating unit's ability to function.

Vital Functions

Critical business processes identified below are the vital functions believed to be most critical to the continuity of Central Georgia Technical College.

OFFICE	VITAL FUNCTION	ALLOWABLE DOWNTIME	PRIORITY LEVEL
President	Emergency Communication	0-24 Hours	High
President	External Communication	0-48 Hours	High
President	Non-Academic Activities	48+ Hours	Low
Executive Vice President	Public Information	0-24 Hours	High
Academic Affairs	Classroom Instruction	24-72 Hours	High
Academic Affairs	Distance Instruction	24-48 Hours	Medium
Academic Affairs	Computer Classroom Instruction	24-72 Hours	Medium
Academic Affairs	Laboratory Instruction	24-72 Hours	Medium
Academic Affairs	Live Work Laboratory's	24-72 Hours	Medium
Academic Affairs	Library Services	48-96 Hours	Low
Facilities/Plant Op	Utilities	0-24 Hours	High
Facilities/Plant Op	Facilities Repair	0-24 Hours	High
Facilities/Plant Op	Cleanup	0-24 Hours	High
Facilities/VP	Fleet Management		Medium
Ancillary Services/VP	Food Service, Vending		Medium
Facilities/VP	Risk Management	0-24 Hours	High
Police Department	Police and Security	0-24 Hours	High
Emergency Management	Emergency Services	0-24 Hours	High
Technology	Core IT systems	0-24 Hours	High
Knowledge Management	Banner/Website	0-24 Hours	High
Administrative Financial Services	Payroll	0-48 Hours	High
Administrative Financial Services	General Accounting Services	24-48 Hours	Medium
Administrative Financial Services	Procurement	0-24 Hours	High
Administrative Financial Services	Mail Services/Shipping/Receiving	48-96 Hours	Medium
Administrative Financial Services	Bookstore	48-96 Hours	Medium
Adult Education	Admissions	24-48 Hours	High
Adult Education	Classroom Instruction	24-72 Hours	High
Adult Education	Distance Instruction	24-48 Hours	Medium

OFFICE	VITAL FUNCTION	ALLOWABLE DOWNTIME	PRIORITY LEVEL
Student Affairs	Admissions	24-48 Hours	High
Student Affairs	Registration	24-48 Hours	High
Student Affairs	Testing	24-48 Hours	High
Student Affairs	Career Services	24-48 Hours	Medium
Student Affairs	Special Populations/ADA	24-48 Hours	High
Student Affairs	Transcript Issuance	24-48 Hours	Medium
Student Affairs	Student Appeals/Grievances	24-48 Hours	Medium
Student Affairs	Grades	24-48 Hours	High
Student Affairs	Athletics/Facilities Rental	48-96 Hours	Medium
Student Affairs	Student Activities	46-98 Hours	Low
Student Affairs	Non-Academic Activities	46-98 Hours	Low
Student Financial Services	Financial Aid		High
Economic Development	Classroom Instruction	24-72 Hours	High
Economic Development	Distance Instruction	24-48 Hours	High
Economic Development	Facilities Rental	48-96 Hours	Medium
Satellite Operations	Classroom Instruction	24-72 Hours	High
Satellite Operations	Distance Instruction	24-48 Hours	High
Satellite Operations	Facilities Rental	48-96 Hours	Medium
Satellite Operation s	Internal Coordination w Various Dept.	0-24 Hours	High
Institutional Effectiveness	Accreditation	42-72 Hours	High

III. RISK ASSESSMENT

The potential hazards or threats that could affect Central Georgia Technical College were determined along with assessing the likelihood of their occurrence, and analyzing the vulnerability. More time and resources are spent planning for and, where possible, preventing disasters that are judged to have both a high likelihood of occurrence and a high level of severity.

This risk analysis addressed the likelihood of occurrence and severity of threats as viewed from a campus wide perspective. Operating units used this assessment as a guide in developing their specific risk assessments, realizing both likelihood of occurrence and event consequence may differ when viewed from a unit level.

Broad Categories of Hazards

Central Georgia Technical College recognized that the planning process must address each hazard that threatens the College. The Technical College is vulnerable to a wide range of threats. The College, with its varying topography, mixed use of space, rapidly growing student population, and transient and recreational population is subject to a wide variety of negative impacts from natural and technological hazards. The natural hazards and technological or man-made hazards that confront the College include:

Natural Hazards
- Floods
- Fires
- Extreme weather (hurricane, tornado, lightening)
- Earthquake

Technological/Man-made Hazards
- Utility/telecomm failure
- Structural Collapse
- Major Fire
- Hazardous materials
- Major vehicle accident
- Major Automobile accident
- Train accident
- Airplane crash
- Disease Outbreak
- Active Intruder
- Hostage Situation
- Public Assembly Emergency
- Civil disturbance
- Terrorism

A threat assessment that depicts the likelihood of occurrence, business continuity and financial impact of each of these hazards is listed below.

Threat Assessment

A threat assessment that depicts the likelihood of occurrence, severity level and financial impact of each of these hazards is listed below.

Threat	Likelihood			Business Continuity Impact			Financial Impact		
	[redacted]	Med	Low	[redacted]	Med	Low	[redacted]	Med	Low
Natural									
Tornado		x		x			x		
Flood			x	x			x		
Hurricane			x	x			x		
Lightening	x			x				x	
Earthquake			x			x	x		
Manmade/Technical									
Structural Collapse			x		X		X		
Utility Failure	X			X				X	
Power Failure	X			X			X		
Telecomm Failure		x		X			X		
Major Fire		x			X		X		
Train Accident			x			X			X
Major Auto Accident	X					X		X	
Air Crash			x			X		X	
Disease Outbreak		x				x		X	
Civil Disorder			x	X				X	
Terrorist Threat		X		X			X		
Hazmat	X			X			X		
Active Intruder			x	X					x
Public Assembly Emergency			x	X				x	
Hostage Situation			x	X					X

IV. RISK MANAGEMENT/CONTINUITY PLANNING

Policy

The President designated a Business Continuity Planner to work directly with the Vice Presidents in creating the Business Continuity plan in coordinating the determination of units with operating processes that are critical and ensuring those processes are identified in section II of this plan.

The Business Continuity Planner will ensure that operating units responsible for critical business processes identified in section II. This documentation enables the operating unit to continue to perform those critical functions and services in the event of a disaster. The College may determine the degree to which continuity planning is consolidated across multiple departments within different areas of the College. This decision will be based on factors such as commonality of business process, size of the division, etc. However, all identified critical processes must be covered by a Worksheet.

Departments must take into account the possibility that a College-wide interruption may affect multiple units. Departments that depend on other departments or external suppliers to provide its critical functions should coordinate with those departments or external suppliers to ensure these suppliers or units also have a continuity plan.

Vice Presidents will provide central coordination of the continuity planning process to assist units in determining space, equipment, and services that might be available within the College and to make the planning process coherent across units.

The Technical College System of Georgia's central office will be responsible for collecting all Technical College plans and worksheets. The combination of this document, and the input of said information in the Living Disaster Recovery Planning System (LDRPS) system will constitute Central Georgia Technical College's complete Business Continuity Plan.

V. UNIT PLAN TESTING AND MAINTENANCE

Testing

Unit Business Continuity Plans must be exercised at a minimum of once every two years.
This exercise will include the following:

- Identifying exercise objectives
- Conducting exercises to validate the viability of the plan
- Documenting exercise results and the steps proposed to correct any problems
- Making appropriate changes to the plan

Training

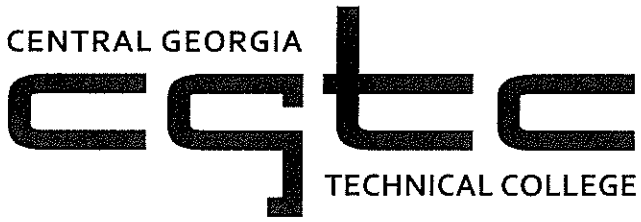
Units will assure that training on the use of the plan is provided to ensure that all staff are adequately trained to fulfill their responsibility in support of the recovery process.
Training for new employees should be carried out within 120 days of their start date.

Plans should be reviewed by the unit head once per year. In particular, the unit head should assure that:

- Critical functions have been identified
- Continuity and recovery strategies are in place
- Documentation for the plan is current
- Minimum levels of required operation and recovery time frames have been set
- Exercising of the plan has been completed during the last 24 months

Plan Maintenance

Vice Presidents must evaluate the impact of changes within the unit, make appropriate plan updates, and communicate changes to persons holding copies of the plan.



CENTRAL GEORGIA TECHNICAL COLLEGE BUSINESS CONTINUITY PLAN

Appendices

Appendix A - Emergency contacts

Emergency contacts include all persons with copies of the plan. Several people work at off-site facilities with immediate availability.

CGTC Emergency Contacts			
Position	Extension	Cell	Alternate
President	3501	542-4612	N/A
Executive Vice President	3333	550-4238	397-6509
Chief of Police	3323	397-5224	397-5224
Police Lieutenant	3453	365-4968	N/A
Police Officer	3453	365-5410	N/A
Police Officer	3453	214-0273	N/A
Police Officer	3453	365-5060	N/A
Police Officer	3453	214-7333	N/A
Envir. Health, Safety & Emerg Mgt Specialist	3436	733-2796	N/A
Vice President, Facilities	3506	550-4023	960-3257
Program Assistant, Facilities	2506	954-1108	N/A
Director of Facilities	3579	214-0943	737-9973
Maintenance Supervisor, North	3441	214-0046	477-9011
Maintenance Supervisor, South	3347	919-4712	N/A
Custodial Services Supervisor North	2516	501-0065	N/A
Custodial Services Supervisor South	3280		N/A
Vice President, Information Technology	3498	731-8289	N/A
Director of Educational Technology	3425	733-0720	N/A
Director of Information Technology	3301	919-5816	N/A
Assistant VP for Knowledge Management	3300	919-1443	397-2527
Asst VP for Marketing/PR	3319	542-4613	229-938-7877
Vice President, Academic Affairs	3510	542-4609	N/A
Asst VP for AA North	3430	955-2786	986-1109
Asst. VP for AA South	3366	231-1271	N/A
Vice President, Student Affairs	3508	396-6228	N/A
Assistant Vice President, Student Affairs	3316	951-0367	N/A
Vice President, Adult Ed.	3288	396-6259	N/A
Assistant VP, Adult Ed	6667	747-4930	N/A
Vice President, Satellite Operations North	2301	550-4051	454-8214
Director, Putnam Co. Center	706-923-5002	706-816-3835	478-457-6632
Director, Crawford Co. Center	836-6024	283-0318	957-6533
Vice President, Satellite Operations South	3298	733-4874	N/A
Director, Hawkinsville Workforce Dev Ctr.	783-3017		
Vice President, Economic Development	3551	550-4501	747-8002
Vice President, Inst. Effectiveness	3514	733-2647	N/A
Executive Director, Human Resources	3700	918-4677	N/A
Asst VP for Advancement	3467	550-5183	476-9837
VP Admin Financial Services	3330	542-4617	N/A
VP Student Financial Services	3414	7315211	365-7795

Appendix B – Administrative Services Analysis

The following plan was prepared in response to a requirement by the Georgia Department of Audits and includes a detailed analysis of the college's business office efforts in prevention of and in case of an emergency situation.

Appendix - Essential Functions for Administrative Services

The essential function of Finance and Administration and minimum number of employees required to perform each function include:

Function	Minimum # of Employees Required
Purchasing	1
Payroll	1
Human Resources	1
Bookstore/Cashiers	2
Accounts Payable	1
Accounts Receivable	1
	7

Critical functional areas prepared individual contingency plans included in this document.

PURCHASING EMERGENCY RESPONSE

Procurement

- Emergency procurement is defined by State Purchasing as "the acquisition of commodities or services, which if not immediately initiated, will endanger human life or health, state property, or the functional capability of a state agency."
- Process procurements as prescribed by State Purchasing
- Maintain supply of blank or pre-printed purchase order forms
- Purchase orders may be typed or hand written on a temporary basis
- Manually number documents following current procedure for non standard documents
- Maintain an Excel spread sheet with sufficient elements and information to facilitate manual reentry (short term emergency) or upload to PeopleSoft electronically (long term crisis)

Staffing

- If current office is functional, entire staff shall report for duty and decisions will be made for job duties and continued reporting based on extent and duration of emergency/crisis
- If current office is not functional, essential staff (Vice President of Administrative Services and the Director of Accounting) will report for duty. Remaining staff will be placed on stand by.

Location

- Current offices if functional

- Temporary site on campus if needed and available
- Off site if necessary (i.e.: Another Technical School, TCSG offices)

Cash flow concerns:

Cash in the bank
Immediate cash outlay (emergency expenses)
Cash receipts (emergency relief funds, etc.)

We would have to make sure that our operating account remained fully accessible to at least three different people with security to make decisions in the absence of one or both of the other two. Our three points of contact for Wells Fargo are: Ivan H. Allen, Michelle Siniard and Alaina Bennett.

Disaster Recovery Plan for Cashiers

I. Accepting Payments
Run an access query program to identify all accounts that have a balance and download into an Excel spreadsheet. The columns will be ID number, last name, first name, amount owed, any flags that the account may have, third party payments, current charges, and several columns for amount paid. When a student inquires about the balance owed we can use this spreadsheet to provide answers. When a student makes a payment we can post the amount of the payment in the
"Amount Paid" column. A hand-written receipt will be given to the student.

II. Fee Assessment
Once the student is registered by Student Affairs the student will bring a paper copy of their schedule to the Bookstore and charges will be calculated and input into a column titled "Current Charges" on the spreadsheet mentioned above. A worksheet will be prepared to help calculate these charges.

III. Billing
Student bills will be produced by using the mail merge feature in Microsoft Word. The data will come from the spreadsheet mentioned above.

IV. Departmental Deposits
Deposits will be verified and a hand-written receipt will be given to the person making the deposit. A spreadsheet will be maintained with the date of the deposit, the amount of the deposit, and the person making the deposit.

V. Third Party Sponsorships and Tuition Discounts
These adjustments will be calculated and posted to the spreadsheet mentioned above.

Disaster Recovery Plan for Accounts Payable

When the College is faced with a loss of its information system or an emergency, bills will still need to be paid. Contractors will require payment. Speakers coming on campus will need to be paid. Requests for payment can be made by direct pay request, and checks typed (written if necessary) and signed.

1. Make sure everyone is physically OK. Locate everyone.
2. Employees should notify the supervisor by phone, email or voice mail that they will not be coming in.
3. Manual checks are located in the vault in Administrative Services.
4. Wells Fargo will have to be notified that we will be using manual checks.
5. If the main check signers are not available, then alternates will need to be arranged.
6. Payments can be made by check requests. Check requests should include proper documentation, authority, and accounts to charge the check to. Copies of the appropriate backup should be attached to the check requests. The carbon copy of the check will be attached to the backup.
7. Payment can be made against an existing purchase order. A manual matching of the invoice against the purchase order will be performed.
8. The Director of Accounting will have the proper cash balance from the day prior. Should that not be available, Wells Fargo should be able to give a fairly accurate balance. A check register will be kept keeping a running total of that balance as checks are written. The check register will indicate the vendor and the amount paid.
9. Once PeopleSoft is running, all invoice documents are entered into the system. From this process a document number is obtained. All manual checks can then be matched to these document numbers. The "manual check" option will have to be checked.

All the above can be run on a laptop if one is available. Spreadsheets can be used to record the check register.

The length of time needed to enter data into the system is totally dependent on the time of the outage and availability of the system during that crisis period.

Disaster Recovery Plan for Accounts Receivable

Just as our vendors still want to be paid during a crisis, we need to ensure that any payments owed to us are received.

1. An AR Outstanding Register is run and printed every two weeks. This can be used in conjunction with the paper invoice copies to determine items not included on the list.
2. Handwritten or typed invoices can be sent out.
3. A spreadsheet needs to be used listing the date, invoice number, customer and amount of each manual invoice.
4. The spreadsheet needs to include columns for date payment received and check number.
5. Once PeopleSoft is running, all manual invoices will be entered into the system and payments made against those invoices will be posted.

Appendix C – Technology Analysis

The following plan was prepared in response to the Gramm-Leach-Bliley Act and the FTC Safeguards Rule and includes a detailed analysis of the college technology effforts in prevention of and in case of an emergency situation.

GRAMM-LEACH-BLILEY ACT AND THE FTC SAFEGUARDS RULE

CENTRAL GEORGIA TECHNICAL COLLEGE INFORMATION SECURITY PLAN

TABLE OF CONTENTS

I. EXECUTIVE OVERVIEW

A. What is the Gramm-Leach-Bliley Act?

The Gramm-Leach-Bliley Act (GLBA) requires —financial institutions‖ as defined by the Federal Trade Commission (FTC), to protect and secure customer information such as names, social security numbers, addresses, account and credit card information. The GLBA also establishes a Safeguards Rule that requires the Technical College to protect and safeguard customer information.

B. What is the FTC Safeguards Rule?

The Safeguards Rule requires financial institutions to secure customer information. It requires the Technical College, as a financial institution, to develop a written information security plan that describes its program to protect customer information.

C. Why does the GLBA apply to Central Georgia Technical College?

The GLBA applies to the Technical College because the Technical College is considered a —financial institution‖ due to the financial activities in which it engages, such as processing students' financial aid.

D. What is the Scope of this Security Plan?

This Plan applies to all —customer information‖ which is defined as any personally identifiable, nonpublic information that the Technical College handles or maintains about an individual in the process of offering a financial product or service, or such information provided to the Technical College by another financial institution. Such customer information is covered whether it is in paper, electronic or other form. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package and other miscellaneous financial services. Examples of customer information include addresses, phone numbers, bank and credit card information, income and credit histories and social security numbers.

D. What are the Primary Goals of this Security Plan?

The primary goals of this Security Plan are to:

Ensure the security and confidentiality of covered data and information; Protect against anticipated threats or hazards to the security or integrity of such information; and

Protect against unauthorized access to or use of covered data and information that could result in substantial harm or inconvenience to any customer.

This Information Security Plan also provides for mechanisms to:

Identify and assess the risks that may threaten covered data and information maintained by Central Georgia Technical College;

Develop written policies and procedures to manage and control these risks;

Implement and review the plan, through, among other measures, an internal audit of all security measures; and

Adjust the plan to reflect changes in technology, the sensitivity of covered data and information and internal or external threats to information security.

II. COMPLIANCE MEASURES

A. Designation of Program Officer

The Information Security Officer is designated as the Program Officer who shall be responsible for coordinating and overseeing the Policy. The Program Officer may designate other representatives of departments within the Technical College to oversee and coordinate particular elements of the Policy. Any questions regarding the implementation of the Program or the interpretation of this document should be directed to the Program Officer or his or her designees.

B. Identifying and Assessing the Risks to Customer Information in Relevant Areas of the Technical College

Every CGTC department that handles or maintains customer information is responsible for identifying the type of information, the form of the information and the security risks within their department and taking appropriate measures to mitigate those risks.

Central Georgia Technical College recognizes that it has both internal and external risks. These risks include, but are not limited to:

Unauthorized access of covered data and information by someone other than the owner of the covered data and information

Compromised system security as a result of system access by an unauthorized person

Interception of data during transmission

Loss of data integrity

Physical loss of data in a disaster

Errors introduced into the system

Corruption of data or systems

Unauthorized access of covered data and information by employees

Unauthorized requests for covered data and information

Unauthorized access through hardcopy files or reports

Unauthorized transfer of covered data and information through third parties

Central Georgia Technical College recognizes that this may not be a complete list of the risks associated with the protection of covered data and information. Since technology growth is not static, new risks are created regularly. Accordingly, the Program Officer will actively participate in staff development sessions and communicate with the DTAE's Information Technology department regarding identification of new risks.

C. Evaluating the Effectiveness of the Current Safeguards in Place

Current safeguards taken to protect customer information include the following:

Description

Computer access limited by system ID's and passwords

Paper reports in file cabinets accessible only to staff in office who need access

Offices that are locked after hours

Data backed up nightly

Passwords that expire periodically and employees must then reset them

Passwords not posted in publicly viewable places

Intrusion detection systems that monitor the Technical

College network to allow the prompt detection of attacks and intrusions

Vulnerability scanning of systems containing customer information

Antivirus protection maintained on computer systems

Firewalls installed on computer systems

Separation of customer information from recycling and shredding of those records

Referring calls or other requests for customer information to designated individuals and being alert to fraudulent attempts to obtain this information

Keeping customer information stored in appropriate filing cabinets and clear of areas with public access

Customer information accessible only by staff with —need to know‖

The effectiveness of the above safeguards is dependent upon

Universal application throughout the Technical College

Technical College employees being responsible for complying with the above safeguards

Implementation of additional safeguards as described below

D. Implementing Supplemental Measures

Additional safeguard measures that are recommended to supplement current safeguards include the following:

Description

Lock file cabinets containing customer information and maintain a list of persons with access to the locked cabinets

Designate a staff member to supervise the disposal of records containing customer information in accordance with the Georgia Secretary of State's Records Retention Rules

Use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information

When providing copies of information to others, remove non-essential and personally identifiable information that has no relevance to the transaction

Erase all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contain customer information in accordance with the Georgia Department of Administrative Services' rules regarding computer inventories

Have the Program Officer conduct security reviews to identify whether additional security measures are required to protect customer information processed and stored on University computer systems

Avoid leaving computer terminals unattended when personally identifiable information is on the screen.

Position or adapt computer terminal monitors so that personally identifiable information is visible only to the authorized user of the terminal

Maintain inventories of all computer systems

Reduce paper forms and documents through increased web access to this information or through internal digital imaging or document managing

Fax machines should be in a secure or supervised area, off limits to unauthorized persons. The use of fax machines should be restricted to authorized personnel only.

Ensure the security of password protected voice mail systems.

Ensure precautionary measures are taken when discussing personal or confidential information over the telephone.

Centralized files.

Off-site storage retention of critical files and documents.

Implement measures to ensure unauthorized persons cannot access University computer systems when left unattended.

E. Social Security Numbers

While the Central Georgia Technical College Information Security Plan discourages the usage of social security numbers as student identifiers, it recognizes that the work is currently underway on the Banner Web system to change from social security numbers as student identifiers to randomly assigned student identification numbers. Therefore, by necessity, student social security numbers still remain in the Central Georgia Technical College student information system. Social security numbers are considered protected information under both the Gramm-Leach-Bliley Act and the Family Educational Rights and Privacy Act (FERPA). The Program Officer will conduct an assessment to determine who has access to social security numbers, in what systems the numbers are used, and in what instances students are being asked to provide a social security number. This assessment will cover Central Georgia Technical College employees as well as possible subcontractors, for example, the bookstore and food services. The Program Officer will maintain a written record of this assessment to assist in the continuing evaluation and adjustment of this plan. (See Section VII below.)

III. EMPLOYEE EDUCATION AND TRAINING

A. Brochure – Information Security Guidelines

An electronic brochure entitled **The Gramm-Leach-Bliley Act: Information Security Awareness Training** will be produced by DTAE to advise employees of their responsibility to protect customer information and university computer systems from unauthorized access and compromises.

B. Departmental Procedures

In conjunction with and with the assistance of DTAE, the Departments that process or maintain customer information are responsible for conducting training for employees who handle such information in the course of their job duties. This training should include physical handling and disposition of non-electronic documents containing customer information as well as proper procedures to follow in processing and storing electronic information and documents.
References of new employees working in areas that regularly work with covered data and information (Cashier's Office, Registrar, Development and Financial Aid) are checked. During employee orientation, each new employee in these departments will receive proper training on the importance of confidentiality of student records, student financial information, and other types of covered data and information. Each new employee is also trained in the proper use of computer information and passwords. Training also includes controls and procedures to prevent employees from providing confidential information to an unauthorized individual, including —pretext calling‖ * and how to properly dispose of documents that contain covered data and information. Each department responsible for maintaining covered data and information is instructed to take steps to protect the information from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures. Further, each department responsible for maintaining covered data and information should coordinate with the DTAE Information Security Office and the Office of Legal Services on an annual basis for the coordination and review of additional privacy training appropriate to the department. These training efforts should help minimize risk and safeguard covered data and information security. These training measures will be applicable, to the extent necessary, to all work study students. All personnel and work study students who have been given the informational brochure and who have received training regarding the Information Security Plan should sign an acknowledgement that that person has received information and training on the Plan . The statement should further acknowledge that the person is aware of, understands his or her responsibility, and agrees to adhere to the plan when dealing with confidential, nonpublic information.

*—Pretext calling‖ occurs when an individual improperly obtains personal information of Technical College students so as to be able to commit identity theft. It is accomplished by contacting the Technical College, posing as a customer or someone authorized to have the customer's information, and through the use of trickery and deceit, convincing an employee of the Technical College to release customer identifying information.

IV. OVERSEEING SERVICE PROVIDERS

The Technical College will take reasonable steps to select and retain service providers who maintain appropriate safeguards for customer information to which the provider has access. The current plan recognizes that, pursuant to 16 C.F.R. § 314.5(b), all contracts entered into prior to June 24, 2002, satisfy the provisions of the Safeguards Rule until May 24, 2004, even if the contract does not include a requirement that the services provider maintain appropriate safeguards. After May 24, 2004, all contracts with service providers who have access to covered information must include a privacy clause and must be in compliance with the GLBA.
For all of those contracts that that do not fall within the above grandfathering provision, the Office of Legal Services will take steps to ensure that all relevant contracts include a privacy clause and are in compliance with the GLBA. A template addendum to any existing contract will be provided by the Office of Legal Services.

V. PHYSICAL SECURITY

Central Georgia Technical College has addressed the physical security of covered data and information by limiting access to only those employees who have a business reason to know such information. For example, personal customer information, accounts, balances and transactional information are available only to Central Georgia Technical College employees with an appropriate business need for such information. Loan files, account information and other paper documents are kept in file cabinets, rooms or vaults that are locked each night. Only authorized employees know combinations and the location of keys. Paper documents that contain covered data and information are shredded at time of disposal.

VI. INFORMATION SYSTEMS

The FTC defines information systems as including network and software design, and information processing, storage, transmission, retrieval and disposal. Guidelines on how to maintain security throughout the life cycle of customer information—from data entry to data disposal are as follows:

> In order to protect the security and integrity of the Technical College network and its data, the Program Officer will develop and maintain a registry of all computers attached to the Central Georgia Technical College network. This registry will include, where relevant, IP address or subnet, MAC address, physical location, operating system, intended use (server, personal computer, lab machine, dorm machine, etc.), the person, persons, or department primarily responsible for the machine, and whether the machine has or has special access to any confidential data covered by relevant external laws or regulations.
>
> The Program Officer assumes the responsibility of assuring that patches for operating systems or software environments are reasonably up to date, and will keep records of patching activity. The Program Officer will review its procedures for patches to operating systems and software, and will keep current on potential threats to the network and its data. Risk assessments will be updated quarterly.

† 16 C.F.R. § 314.4(b) *et. seq.*:

. . .

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations,
including:
(1) Employee training and management;
(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.
(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
(d) Oversee service providers, by:
(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
(2) Requiring your service providers by contract to implement and maintain such safeguards.
(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program. \\cgtcdepartment\domain_documentation\Policy\CGTC\Safeguards_Plan.doc 9

The Program Officer bears primary responsibility for the identification of internal and external risk assessment, but all members of the Central Georgia Technical College community are involved in risk assessment. The Program Officer, working in conjunction with the relevant Central Georgia Technical College offices, will conduct periodic risk assessments, including but not limited to the categories listed by the Gramm-Leach-Bliley Act.†

The Program Officer, working in cooperation with relevant Central Georgia Technical College departments, will develop and maintain a data handbook, listing those persons or offices responsible for each covered data field in relevant software systems (financial, student administration, etc.). The Program Officer and the relevant departments will conduct ongoing audits of activity, and will report any significant questionable activities.

The Program Officer will work with the relevant offices (Human Resources, the Registrar and Financial Aid, among others) to develop and maintain a registry of those members of the Central Georgia Technical College community who have access to covered data and information. The Program Officer, in cooperation with Human Resources and other relevant offices will work to keep this registry up to date.

The Program Officer will assure the physical security of all servers and terminals which contain or have access to covered data and information. The Program Officer will work with other relevant areas of Central Georgia Technical College to develop guidelines for physical security of any covered servers in locations outside the central server area.

The Program Officer will, to the extent feasible, develop a plan to ensure that all electronic covered information is encrypted in transit and that the central databases are strongly protected from security risks

VII. MANAGING SYSTEMS FAILURES

Students should be notified promptly if their nonpublic personal information is subject to loss, damage, or unauthorized access. The school will provide all students of compromised information with a written notice describing the compromised information. If the school is unable to specify what information was compromised or is unable to identify the students owning the compromised information, then the school will provide a notice to its general student population giving the probable dates and a general description of possible information that has been compromised. The notice should provide a contact number by which concerned students can discuss the compromise with the school.

VIII. CONTINUING EVALUATION AND ADJUSTMENT

This Information Security Plan will be subject to periodic review and adjustment. The most frequent of these reviews will occur within Information Technology, where constantly changing technology and evolving risks mandate increased vigilance. Continued administration of the development, implementation and maintenance of the program will be the responsibility of the designated Program Officer who will assign specific responsibility for Information Technology implementation and administration as appropriate. The Program Officer, in consultation with DTAE's Information Security and the Office of Legal Services, will review the standards set forth in this policy and recommend updates and revisions as necessary. It may be necessary to adjust the plan to reflect changes in technology, the sensitivity of student/customer data and internal or external threats to information security.

IX. CONCLUSION AND ENFORCEMENT

Many privacy abuses are the result of carelessness and errors by those who handle confidential, nonpublic information. Some are caused by inadequate security. Responsible information-handling practices begin with the implementation of the safeguard measures within this plan. Failure to implement and apply the required measures, or disregard of the implemented measures, may result in disciplinary action.