

Division of Administrative and Information Services

Business Continuity Planning for Information
Technology Systems

DATC
a UCAT Campus

May 2011

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
SECTION I: THE BUSINESS CONTINUANCE PLAN (BCP)	5
Section I.A: Payroll	5
Section I.B: Financial Information Systems	7
Section I.C: Bookstore	10
Section I.D: Student Services/Student Management System.....	11
Section I.E: Training Division and Instruction	15
SECTION II: THE CONTINUITY OF OPERATIONS PLAN (COOP) AND OVERVIEW	16
Damage Assessment	16
Information Technology Services Recovery Team.....	16
Locate and Salvage Data and Equipment	16
Designate Recovery Site.....	17
Remote Recovery Site.....	17
Restoring Systems.....	17
Network Infrastructure.....	18
Systems/Platforms Recovery	18
Restore the Directory	18
Mission Critical System Applications Installed	18
Restore Application Databases.....	18
Client Access to Applications and Peripherals.....	18
Move Back to Restored Permanent Facility	18
Replacement Equipment.....	19
Installations Disks	19
Systems Documentation	19
Backups	19
SECTION III: THE CONTINUITY OF OPERATIONS PLAN (COOP) PROCEDURES	21
I. Damage Assessment.....	21
II. Information Technology Services Recovery Team	21
III. Locate and Salvage Data and Equipment.....	21
IV. Designate Recovery Site	21

V.	Restoring Systems.....	22
VI.	Network Infrastructure	22
VII.	Systems/Platforms Recovery	23
VIII.	Restore the Directory.....	23
IX.	Mission Critical System Applications.....	23
X.	Restore Application Data	23
XI.	Client Access to Applications and Peripherals.....	24
SECTION IV: CYBER INCIDENT RESPONSE PLAN		25
	Computer Crime	25
	Preventative Measures.....	25
	Computer Crime Recovery Procedures	25
APPENDIX A: VENDOR CONTACTS		26
APPENDIX B: REPLACEMENT EQUIPMENT		27

Executive Summary

Primary Focus of the Plan

Over the years, dependence upon the use of computing devices in the day-to-day business activity at DATC has become the increasing standard. In the event of a disaster, the normal use of the various mission critical applications may be affected to some degree. Without adequate planning and preparation to deal with unplanned and undesired events, DATC's central computing services could be unavailable for an extended period of time. Business continuity planning is designed to mitigate the risk of system and service unavailability by focusing effective and efficient recovery solutions.

Therefore, the primary focus of this document is to provide a plan to respond to any unplanned loss of College services or any business disruption that interrupts, destroys, or severely cripples the ability for DATC business unit's to perform normal day-to-day operations. The intent is to restore operations as quickly as possible in either a centralized or in a remote location with the latest up-to-date data available.

This IT Business continuity planning guide identifies fundamental planning principles and practices to help personnel develop and maintain effective IT business continuity plans. This plan outlines planning principles that may be applied to a wide verity of incidents that could affect IT system operations.

The Business Continuance Plan (BCP)

The BCP focuses on sustaining an organization's business functions during and after a disruption. Specifically, the BCP addresses the following business functions:

1. Procedures to process Payroll
2. Procedures to process Financial Information Systems
3. Procedures to resume Bookstore Services
4. Procedures to process Student Services/Student Management Systems
5. Procedures to resume College Instruction

The Continuity of Operations Plan (COOP)

The COOP presents an orderly course of action overview 1) to assess damage 2) to restore critical computing capability 3) and to decide whether to repair the affected site or select a predetermined alternate site for recovery. If damage is severe enough and the determination is made to rebuild the primary site or move to an alternate site, the COOP outlines procedures to execute the plan to restore critical computing capability.

The COOP Procedures

The COOP Procedures outlines steps to restore systems in an orderly and precise fashion. When the COOP Procedures are complete, systems are available for use.

The Cyber Incident Response Plan

The Cyber Incident Response Plan establishes procedures to address cyber attacks against an organization's information technology system(s). These procedures are designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized

access to a system or data (e.g. malicious logic, such as a virus, worm, Trojan horse, or any form of malware).

Section I: The Business Continuity Plan (BCP)

The BCP focuses on sustaining an organization's business functions during and after an interruption of services. Each section contains plans developed by respective business units/organizations and will be updated on a regular basis by the same respective business units/organizations.

Section I.A: Payroll

Business Resumption Goal:

To generate payroll checks / direct deposits, benefit and deduction checks even though the production system at DATC not operable. If the payroll system (Great Plains) is not available, payroll direct deposits and paychecks will be processed at other locations from file copies of the previous payday's payroll direct deposits and paychecks. The intent is to restore operations as quickly as possible with the latest and most up-to-date data available. Since Payroll is processed monthly, the time of the month that the system is down would be critical in determining exactly what steps should be taken.

ADP

Short Term (day or two)

If the payroll system was down for a day or two during the first three weeks of the month, there would be minimal impact. Most payroll transactions could wait. Manual procedures could be followed to make critical items happen.

If the payroll system was down for a day or two during the last week before payroll was due. Processing of the payroll would take place through ADP. Access to ADP systems could be granted to off-campus (Davis Business Alliance and Freeport) sites for payroll processing and ADP backup. Restoration could be done through ADP backup. Follow manual procedures to make items happen that have not been entered into the ADP systems and to process critical items.

Intermediate (up to two weeks)

If the payroll system was down for a week or two during the first three weeks of the month, there would be minimal impact. Most payroll transactions could wait. Follow manual procedures to make critical items happen.

If the payroll system was down during the last week before payroll was due. Work with ADP to process payroll until payroll system is back up. Access to ADP systems could be granted to off-campus sites (Davis Business Alliance and Freeport) for payroll processing and ADP backup. Restoration could be done through ADP backup. Follow manual procedures to make items happen that have not been entered into the ADP systems and to process critical items.

Extended (longer than two weeks)

Work with ADP to process payroll until payroll system is back up. Access to ADP systems could be granted to off-campus sites (Davis Business Alliance and Freeport) for payroll processing and ADP backup. Restoration could be done through ADP backup. Follow manual procedures to make items happen that have not been entered into the ADP systems and to process critical items.

Microsoft Dynamics Great Plains Accounting System

Short term (a day or two)

Payroll is usually completed a few days prior to the actual deadline, giving a few days cushion.

1. Restore backup from previous night
2. Review for missing information.
3. Process as usual.

Payroll change requests and time sheet information would need to wait until system became available.

Intermediate (one week)

Time card information and payroll change requests could be done manually on paper copies of the electronic forms if information was critical for processing immediately. Otherwise, information could wait until the system became available again.

Store dated backup at Davis Business Alliance and Freeport Center.

1. Take offsite backup to Premier Computing in SLC
2. Use offsite information to get system functioning in SLC office
3. Update with information changes since last offsite backup completed
4. Process as usual.

Extended (longer than one week)

This would imply some type of disaster that would shut down the campus physically. Time card information and payroll change requests could be done manually on paper copies of the electronic forms if information was critical for processing immediately.

Store dated backup at Davis Business Alliance and Freeport Center.

1. Take offsite backup to Premier Computing in SLC
2. Use offsite information to get system functioning in SLC office
3. Update with information changes since last offsite backup completed
4. Process as usual until system could be brought into service at a permanent location.

“Fall Back” Payroll Personnel

Area: Payroll Shelly Nielsen Office: 801-593-2444 Cell: 801-510-2467 Home: 801-773-0667 Other:	Sharon Hokanson Office: 801-593-2326 Cell: 801-336-7850 Home: 801-773-4376 Other:	Jeff Lund Office: 801-593-2307 Cell: 801-971-2132 Home: 801-294-2343	Ric Higbee Office: 801.593.2393 Cell: Home: Other:
--	---	---	--

Section I.B: Financial Information Systems

Business Resumption Goal:

The goal of this business resumption plan is to document the steps necessary to ensure that in the event there is disruption of resources (i.e., computing hardware/software failure, data communications transmission) for an extended period of time, the Financial Information System can still operate.

Accounts Payable Transactions

Very few AP items are critical and can wait for a week if necessary. If items are critical and time sensitive, hand cut checks can be issued and input into the financial system when it becomes available.

Short Term (one to two days)

Minimal impact. Most payable transactions could wait. Follow manual procedures listed below to make critical items happen.

Intermediate (up to two weeks)

Minimal impact. Most payable transactions could wait. Follow manual procedures listed below to make critical items happen

Extended (longer than two weeks)

1. Estimate length of down time
2. Prioritize outstanding payables
3. Payables deemed as critical would be paid through the manual process listed below.
4. If downtime expected to last several months, coordinate with another UCAT entity or consulting group and use system remotely.

Manual procedures:

1. Follow purchasing policy in regards to backup and documentation
2. For items less than \$1,000, use a purchasing card or credit card to cover the cost of the item.
3. For items greater than \$1,000 or when purchasing cards are not a payment option, a manual check will be issued. (A small supply of preprinted check stock will be kept on hand that could be typed or hand written and signed by the appropriate signers on the bank account.

Restoration procedures:

1. Restore latest backup
2. Compare last check number on backup to check register
3. Input any missing Account Payable invoices necessary to create the checks
4. Input any document input but not paid (found in the "waiting for check" accordion file)
5. Record AP checks already processed

Purchase Orders

Emergency Purchase Orders could be cut using the request for Purchase Order form. Using the last PO generated from the system, we could keep a manual log of purchase orders using the next numbers from Great Plains. These PO's could then be recorded in the system when it comes back up.

Payments/Receipts

Short term (Less than one week)

If electricity is not available, hand written receipts would be issued using the supply of pre-numbered receipts. All pertinent information would need to be recorded including customer name, ID #, amount, items being purchased; type of payment and cc information is applicable.

If electricity is available but network is not, the stand alone version of Quick Books would be used. The inventory items in Great Plains would be duplicated on Quick books so that receipts generated by Quick Books could be recorded at a later time in Great Plains. End of day procedures for Quick Books would be followed.

Intermediate (up to 4 weeks)

The stand alone version of Quick Books would be used. The inventory items in Great Plains would be duplicated on Quick books so that receipts generated by Quick Books could be recorded at a later time in Great Plains. End of day procedures for Quick Books would be followed.

If electricity were unavailable for more than a few weeks, the school would probably not be open for receipting of tuition and fees.

Long term (more than 4 weeks)

The stand alone version of Quick Books would be used. The inventory items in Great Plains would be duplicated on Quick books so that receipts generated by Quick Books could be recorded at a later time in Great Plains. End of day procedures for Quick Books would be followed.

If electricity were unavailable for more than a few weeks, the school would probably not be open for receipting of tuition and fees.

Restoration Procedures:

1. Restore latest backup
2. Identify the last receipt number generated on the system
3. Input the system generated receipt in Great Plains not in the restored version
4. Do end of day processing as usual
5. Input Quick Books and/or hand receipts in Great Plains, referencing the manual receipt number in the PO field in Great Plains
6. Do end of day processing to match the manual process.

Journal Entries

1. Restore most current backup information.
2. Identify last journal entry input on backup information
3. Using hard copies or scanned copies of journal entries, reenter all journal entries not appearing in the backup.
4. If a month end closing has happened since the last backup, do one month at a time to ensure that the month end reports match with what was reported prior to the system going down.

In the event that anyone or several staff members are not able to participate in the execution business resumption plan, a “fall back” person has been designated to step in and complete the process. Backup plan for staff is as follows:

Area: Fiscal Jeff Lund Office: 801-593-2307 Cell: 801-971-2132 Home: 801-294-2343 Other:	Rosa Diazvela Office: 801-593-2437 Cell: 801-628-4913 Home: 801-544-5362 Other:	Office: Cell: Home: Other:	Office: Cell: Home: Other:
Area: Cashier/ A/R Michael Bruderer Office: 801-599.2313 Cell: Home: Other:	Cathy Salisbury Office: 801-593-2443 Cell: Home: Other:	Jeff Lund Office: 801-593-2307 Cell: Home: Other:	Office: Cell: Home: Other:
Area: Accounts Payable Lauralee Horrocks Office: 801-593-2305 Cell: 801-628-3317 Home: 801-295-5408 Other:	Cathy Salisbury Office: 801.593.2443 Cell: Home: Other:	Rosa Diazvela Office: 801-593-2437 Cell: 801-628-4913 Home: 801-544-5362 Other:	Jeff Lund Office: 801-593-2307 Cell: 801-971-2132 Home: 801-294-2343 Other:

Section I.C: Bookstore

Business Resumption Goal:

The goal of this business resumption plan is to document the steps necessary to ensure that in the event there is disruption of resources (i.e., computing hardware/software failure, data communications transmission) for an extended period of time, the Bookstore can still operate.

In the case of an emergency that would knock out power and Computer Abilities, we would do the following:

Short-term: We would most likely close the store for the short term. The Store would be dark and a hazard for our customers and staff, so closing would be the best solution.

Intermediate: After 1-2 days, we would need to find a way to be open, so we would find a source of lighting for my staff to use in the store, and would take requests from customers for the bookstore staff to retrieve items for customers and record these items on a manual receipt. At this point, I would still not want customers browsing the store due to safety concerns. When power eventually came back up we would record all of these sales in our computer system.

Long-term: If the problem existed for more than 1 week and looked to persist further, we would have to locate some sort of generator system to run a light system and to be able to operate our Pos System. At this point customers would be allowed back in our store.

Section I.D: Student Services/Student Management System

Business Resumption Goal:

The goal of this business resumption plan is to document the steps necessary to ensure that in the event there is disruption of resources (i.e., mainframe hardware/software failure, data communications transmission) for an extended period of time, the management of students can still operate in the manner outlines below.

Essential Personnel – Priority 1, 2, 3 and 4

Name	Job Title	Full Services	Minimal Services w/ Enrollment	Minimal Services w/o Enrollment
Asay, Danna	SS Mgmt Asst	1	1	1
Cummings, Kevin L	Director of Student Services	1	1	1
McMullin, Robyn S.	Registration Spec	1	1	1
Brown, Peggy L	Registration Technician	1	1	2
Convery, Christine R.	Appld Tech Counselor	1	1	2
Hepler III, Albert W.	Appld Tech Counselor	1	2	2
Hill, Holly	Special Needs Tracker	1	1	2
	Appld Tech Advisor	1	2	2
	Diversity Sv Advisor	1	1	2
Wood, Julie	Assessment Technician	1	1	2
Bryson, Julie A	Customer Service Rep	1	2	3
Butler, Jamie	Customer Service Rep	1	2	3
	Customer Service Rep	1	2	3
Leonard, Melanie L	Customer Service Rep	1	2	3
Norman, Shantel	Customer Service Rep	1	1	3
Sherwood, Marie	Assessment Clerk	1	2	3
	Commons Host	1	1	3
	College Operator	1	2	4
Baker, Carrie G.	Freeport Receptionist	1	3	4
Dahl, Emily Hope	Hear Imp Spc Nds Trk	1	2	4
Evans, Ashel A.	Special Needs Tracker	1	2	4
Faiola, Corrin M	Hear Imp Spc Nds Trk	1	3	4
Huesgen, Shirley Mona	Special Needs Tracker	1	3	4
Isaacson, Douglas	Special Needs Tracker/Testing	1	3	4
McCloy, Wendi	Hear Imp Interpreter	1	3	4
McNew, Carol	Freeport Receptionist	1	3	4
Miller, Angela K.	Special Needs Tracker	1	3	4
Muir, Aimee O	Hear Imp Interpreter	1	3	4
Shumway, Joellen H.	CNA Skills Tester	1	3	4
Slater, V Diane	Special Needs Tracker	1	2	4
Smith, Tracie F	College Receptionist	1	2	4
Whitten, Linda M	Center Oprtpr/recpt	1	2	4

Priority numbers indicate the order in which staff members are expected to report for work. In the event that an individual cannot report, the next highest priority person would be asked to report.

Minimum Needs for Initial Response and Beyond

In the hours immediately following a disaster, information could be provided via telephone or cell phone if available. Bulletin boards and other posted written notices could be used to share information with students and other constituents on site.

Once the conditions for the resumption of business have been determined (same facility, new facility, availability of data and voice connections, etc.) appropriate portions of the plan outlined below can be put into place to resume operations.

Internal Communication

Existing radios could be used to facilitate internal communications.

Assessment and Enrollment

The assessments required for enrollment are pencil-and-paper tests which are scored by hand or using a standalone Scantron machine. These could be offered immediately upon the resumption of business.

Other assessments which are computer-based and offered for licensing or other verification purposes would not be immediately available. In the event of a long-term need, vendors and other agencies might make pencil-and-paper versions available. However, administering these assessments would not be a high priority or necessary for regaining minimum functioning for the College.

Enrollment could resume immediately using pencil-and-paper applications which would be verified by enrollment personnel and stored until such time as they could be entered into the Student Information System.

Scheduling

In the short term (less than one week) hand rolls could be kept by classroom instructors and stored in Student Services until such time as the data could be entered into the electronic record-keeping system.

In the medium term (one week to several months) Excel spreadsheets could be assembled from existing paper data sources and used to track new enrollments and daily class rolls. When regular network services resume, the data could be transferred electronically into student record system.

Student Achievement Records

Similar to the rolls, student achievement records could be reconstituted (in the short term) from existing paper documents. Subsequently these could be recorded (temporarily) in standalone spreadsheets which could be accessed on non-networked computers. When full network services resume, data could be transferred into the student system.

Student Records and Archives

The area of business most likely to be impacted by a significant disruptive event would be student records. The majority of these records are stored electronically – either via a scanning system or electronic database records. Many of these records would be inaccessible if the network were down.

Presuming that the server could be made to run – either locally or at the UCAT offices in Salt Lake City, the records could be accessed via a station connected directly to the server. Data and the programs necessary to access the data could be restored (as necessary) for either on-site or off-site back-ups.

Requests for records would be accepted by the Registrar or an alternate and information would be manually retrieved from the available system.

Financial Aid

Local financial aid offerings (scholarships) could continue to be managed locally. Federal and Veterans Aid, which are subject to extensive Federal regulations, would need to be negotiated with the appropriate authorities.

Counseling

Counseling is important service offered by the College. Because it is essentially a human service, a disaster would not necessarily impact the ability to offer this service. Indeed, in the aftermath of some traumatic event, Counselors could serve the College community by offering their services to students who are dealing with the emotional fallout of the catastrophe.

In the event that anyone or several staff members are not able to participate in the execution business resumption plan, a “fall back” person has been designated to step in and complete the process. Backup plan for staff is as follows:

Kevin Cummings. Office: 593-2345 Cell: 499-9520 Home: 774-0680 Other:	Danna Asay Office: 593-2309 Cell: 243-4995 Home: 451-5312 Other:	Office: Cell: Home: Other:	Office: Cell: Home: Other:
Counseling Drew Johnson Office: 801.593.2314 Cell: Home: Other:	Office: Cell: Home: Other:	Office: Cell: Home: Other:	Office: Cell: Home: Other:
Area Assessment Julie Wood Office: 593-2361 Cell: 564-0493 Home: 546-3705 Other:	Marie Sherwood Office: 593-2336 Cell: Home: 479-4774 Other:	Office: Cell: Home: Other:	Office: Cell: Home: Other:

Registrar Robyn Jacobson Office: 593-2420 Cell: 589-9373 Home: 593-9732 Other:	Office: Cell: Home: Other:	Office: Cell: Home: Other:	Office: Cell: Home: Other:
CSRs Shantel Norman Office: 593-2332 Cell: 435-730-5305 Home: Other:	Jamie Butler Office: 593-2301 Cell: 718-9551 Home: 546-6065 Other:	Julie Bryson Office: 593-2301 Cell: 718-9222 Home: 444-2672 Other:	Melanie Leonard Office: 593-2488 Cell: 548-0266 Home: 548-0266 Other:
Peggy Brown Office: 593-2312 Cell: 458-0355 Home: 479-1146 Other:	Office: Cell: Home: Other:	Office: Cell: Home: Other:	Office: Cell: Home: Other:

Section I.E: Training Division and Instruction

Business Resumption Goal:

The goal of this business resumption plan is to document the steps necessary to ensure that in the event there is disruption of resources (i.e., mainframe hardware/software failure, data communications transmission) for an extended period of time, the classroom instruction can still operate.

Short Term – 1-2 days Intermediate – less than 1 week

Shut down College

Call faculty and staff

Designate staff member to print “School Closed” signs and post on campus doors

Long Term – more than 1 week

Shut down College

Call faculty and staff

Designate staff member to print “School Closed” signs and post on campus doors

President/Vice Presidents/Directors decide whether to find temporary class issues.

Section II: The Continuity of Operations Plan (COOP) and Overview

Damage Assessment

To determine how the business continuity plan will be implemented following an emergency, it is essential to assess the nature and extent of the damage to the system. Damage assessment is intended to establish the extent of damage to mission critical computing devices and the facility that houses them as quickly as the given conditions permit, with personnel safety remaining the highest priority. The following areas should be addressed:

- Cause of the emergency or disruption
- Potential for additional disruptions or damage
- Area affected by emergency
- Status of physical infrastructure (e.g., structural integrity of data center, condition of electric power, telecommunications, and heating and ventilation/environmental conditions)
- Inventory and functional condition of IT equipment
- Type of damage to IT equipment or data (e.g., water, fire, physical impact, electrical surge)
- Estimated time to restore normal services

Another primary goal is to determine where the recovery should take place and the condition of computing devices at the disaster site.

Team members should be liberal in their estimate of the time required to repair or replace a damaged resource. Take into consideration cases where one repair cannot begin until another step is completed. Estimates of repair time should include ordering, shipping, installation, and testing.

When considering damaged computing devices, consider first the minimal list of equipment required for the College to operate and function. Separate items into two groups: one group composed of salvageable components to assemble for minimal operation and function; the second group consists of items either missing or destroyed needing replaced at some point in time. These "salvageable" items will have to be evaluated by IT and repaired as necessary. Based on results from this process, acquiring replacements can begin.

With respect to the facility, evaluation of damage to the structure, electrical system, air conditioning, and network infrastructure should be conducted. If estimates from this process indicate that recovery at the original site will require more than 14 days, migration to the cold site should be considered.

Information Technology Services Recovery Team

The Information Technology Services Recovery Team will be led by the IT Director. The team leader will be responsible for selecting the other team members to assist in system and data recovery (it is most likely that all IT personnel will assist). This team will be responsible for overseeing the restoration of the campus network, restoration of systems, and all network connections necessary at the recovery site. Because there is such a high degree of reliance on the campus network for instruction and administrative purposes, very high emphasis must be placed on restoring the network as quickly as possible. Immediately following the disaster, a planned sequence of events begins. A key personnel contact list to execute the plan follows:

Locate and Salvage Data and Equipment

Early efforts are targeted at protecting and preserving the salvageable computer and networking equipment. In particular, any backup/magnetic storage media (hard drives, magnetic tapes, CDs, DVDs) are identified and either protected from the elements or removed to a clean, dry environment away from the disaster site.

Designate Recovery Site

An inspection of the data center and telecommunication closets scene is done by IT personnel to estimate the amount of time required to put the salvageable equipment back into working order, providing there are adequate facilities to work with. A decision is then made whether to use a designated remote location where computing and networking capabilities can be temporarily restored until the primary site is available. If estimates from this process indicate that recovery at the original site will require more than 14 days, migration to remote recovery site should be considered. Work begins almost immediately at repairing or rebuilding the primary site.

Remote Recovery Site

Warm and cold recovery sites are areas physically separate from the primary site where space has been identified for use as the temporary home for the computer and network systems while the primary site is being repaired. The warm and cold sites must have adequate space to house the hardware, with some office space available for operating and technical personnel. It must have good connectivity to the campus fiber optic network. Additionally, a certain amount of preparation must be made for electrical and cooling capacity to support file servers and network equipment.

If estimates from this process indicate that recovery at the original site will require more than 14 days, salvaged and new components are reassembled at the recovery site according to the instructions contained in this plan. Since all plans of this type are subject to the inherent changes that occur in the computer industry, it may become necessary for recovery personnel to deviate from the plan, as computing industry has the propensity to change rapidly. If vendors cannot provide a certain piece of equipment on a timely basis, it may be necessary for the recovery personnel to make last-minute substitutions. After the equipment reassembly phase is complete, the work turns to concentrate on the data recovery procedures.

Cold Site

A remote site located away from the main campus. This site has the capability to become the data center or at least an extension of the data center. It would not contain any equipment that is hot or continuously connected to the data center.

Warm Site

A remote site located away from the main data center. This site has the capability to become the data center or at least an extension of the data center, similar to the cold site. Differing from the cold site, however, this site could possibly contain equipment that is hot but yet a secondary subset of the live equipment and data that resides at the data center.

Restoring Systems

If equipment cannot be salvaged and must be replaced, the recovery process relies heavily upon DATC procurement and vendors to quickly provide replacements for those damaged resources.

Data recovery relies entirely upon the use of backups stored locally and in locations off-site from the DATC's main campus. Backups can take on various forms of media including hard drives, magnetic tapes, CDs, DVDs. After identifying salvageable equipment, early data recovery efforts must first focus on restoring the operating system(s) for each file server/computer system. Next, mission critical system data must be restored. After system data is restored, individual user data is restored. At this point, owners of data may need to be involved to ensure that data is restored properly.

Network Infrastructure

It is critical that network connectivity be established within the data center first. Once communications are established within the data center between mission critical network devices, applications, and appliances, connectivity to other telecommunications closets should be established.

Systems/Platforms Recovery

After data center communications are established, it is time to identify usability of file servers, storage devices, and backup/restore devices. Salvage all usable equipment; establish communications to equipment through network routing and switching fabric. If components are deemed unusable or unsalvageable, then work with procurement to order new equipment meeting minimal specifications outlined in Appendix B.

Restore the Directory

After the operating systems have been installed, it becomes necessary that the directory be restored to once again establish user accounts, security, and other essential system objects.

Mission Critical System Applications Installed

Before data can be restored, system applications must be installed and configured. System application installation disks must be preserved and accessible. Once system applications are installed, and the network is repaired, client applications can be installed.

Restore Application Databases

Since it is likely that some time may have elapsed between the time that the off-site backups were made and the time of the disaster, application owners must have means for restoring each running application database to the point of the disaster. They must also take all new data collected since that point and input it into the application databases. When this process is complete, DATC can re-open for business with respect to information technology provided services. Some applications may be available only to a limited few key personnel, while other applications may be available to anyone who can access the computer systems.

Client Access to Applications and Peripherals

Once applications are installed and configured and databases are restored, then next step is to establish and ensure client devices can access system applications and peripherals such as scanners and printers.

Move Back to Restored Permanent Facility

If the recovery process has taken place at an alternate remote site, physical restoration of the DATC data center will have begun. When the data center is ready for occupancy, the systems assembled at the alternate remote site are to be moved back to their permanent home.

Replacement Equipment

This plan contains a complete inventory (Appendix B) of the components of each of the computer and network systems and their software that must be restored after business disruption. The inevitable changes that occur in the systems over time require that the plan be periodically updated to reflect the most current configuration. To avoid problems and delays in the recovery, every attempt should be made to replicate the current system configuration. However, there will likely be cases where components are not available or the delivery timeframe is unacceptably long. Although some changes may be required to the procedures documented in the plan, using different models of equipment or equipment from a different vendor may be suitable to expediting the recovery process.

Installations Disks

A set of all disks or other media used to create initial installation of systems will be stored in a fire safe lock box in the data center and in a fire safe lock boxes remotely in the warm and cold recovery sites.

Systems Documentation

Sets of documentation used to create initial installation of systems and configuration changes from default will be stored in a fire safe lock box in the data center and in a fire safe lock box remotely in the warm and cold recovery sites.

Backups

The data that was stored on the old equipment cannot be bought at any price. It must be restored from a copy that was least affected by the disaster. There are a number of options available to us to help ensure that such a copy of data survives a disaster at the primary facility with varying costs.

Redundant Data Repository

This option calls for a Storage Area Network (SAN) disk subsystem located at a remote site away from the primary data center connected with a high speed Wide Area Network (WAN). This remote redundant SAN is connected to a SAN at the primary data center. Data written to disk at the primary site is automatically transmitted to the remote site. This guarantees that the most current database updates are stored at both primary and remote data centers essentially in real-time. This option is expensive and it does not require that an entire computer system be built at a remote data center, just the disk subsystem. DATC will work to this end although funding availability is very limited.

Automated Off-Site Tape/Disk Backup

This option or level of redundancy calls for a tape subsystem or disk subsystem located at a remote site away from the primary data center connected with a high speed Wide Area Network (WAN). Copies of operating system data, application and user programs, and databases can be transmitted to the remote tape subsystem where it is stored on tape or disk. While this option does not guarantee real-time updates available with the remote dual copy disk option, it does provide means for conveniently taking backups and storing them off-site.

Off-Site Tape/Disk Backup Storage

This option calls for the transportation of backup tapes made from the primary computer facility to an off-site remote location. Survivability of the backups is critical in a disaster, but need quick availability of the backups is also required.

Backup Solutions

System applications and data should be backed up regularly according to policy. Servers can be backed up through a distributed system, in which each server has its own drive, or through a centralized system, where a centralized backup device is attached to one server. Three types of system backup methods are available to preserve server applications and data:

Full

A full backup captures all files on the disk or within the folder selected for backup. Because all backed-up files were recorded to a single media or media set, locating a particular file or group of files is simple. However, the time required to perform a full backup can be lengthy. In addition, full backup of files that do not change frequently (such as system files) could lead to excessive, unnecessary media storage requirements.

Incremental

An incremental backup captures files that were created or changed since the last backup, regardless of backup type, incremental backups afford more efficient use of storage media, and backup times are reduced. However, to recover a system from an incremental backup, media from different backup operations may be required. For example, consider a case in which a folder needed to be recovered. If the last full backup was performed three days prior and one file had changed each day, then the media for the full backup and for each day's incremental backup would be needed to restore the entire folder.

Differential

A differential backup stores files that were created or modified since the last full backup. Therefore if a file is changed after the previous full backup, a differential backup will save the file each time until the next full backup is completed. The differential backup takes less time to complete than a full backup. Restoring from a full backup media and the last differential media would be needed. As a disadvantage, differential backup takes longer to complete than incremental backups because the amount of data since the last full backup increases each day until the next full backup is executed.

Section III: The Continuity of Operations Plan (COOP) Procedures

I. Damage Assessment

Depending on the estimated length of system failure and system recovery time, notification must be made to other College business units so they can execute their plans of business continuance. The extent of the disaster will also determine the initial recovery site.

II. Information Technology Services Recovery Team

When informed, the team leader will contact all members of the recovery team to execute the COOP as outlined.

Contact #1 Greg Scherer Office: 801.593.2455 Cell: 801.698.1724 Home: 801.782.5471 Other:	Data Contact Terri Stephens Office: 801.593.2316 Cell: Home: Other:	Web Contact Andrew Ariotti Office: 801.593.2459 Cell: 309 Home: Other:	
Contact #2 Robert Dysart Office: 801.593.2503 Cell: 801.698.1723 Home: 801.334.8413 Other:	Contact #3 Rich Dunaway Office: 801.593.2432 Cell: 801.698.1701 Home: Other:	Contact #4 Joel McConkie Office: 801.593.2521 Cell: 801.698.0646 Home: 801.292.9745 Other:	Contact #5 (PM) Brent Dalley Office: 801.593.2380 Cell: Home: Other:

III. Locate and Salvage Data and Equipment

- a. Locate backup media containing mission critical data
- b. Re-locate backup media to an environmentally safe location
- c. Separate all equipment into two groups:
 - i. Salvageable components to assemble for basic operation and function
 - ii. Items either missing or destroyed needing replaced at some point in time
- d. Of the salvageable equipment, estimate whether the system can be restored in:
 1. Short term (1 to 2 days)
 2. Intermediate (less than two weeks)
 3. Long term (more than 2 weeks)

IV. Designate Recovery Site

- a. Estimate whether the system can be restored in:
 - i. Short term (1 to 2 days)
 - ii. Intermediate (less than two weeks)
 - iii. Long term (more than 2 weeks)
- b. If the extend of damage to the data center and connectivity to telecommunications closets is can be repaired within 14 days, choose one of the recovery sites for temporary system recovery:
 - i. Option 1: Warm Site Short Term
 The warm site is located in the Roy and Elizabeth Simmons Building (DBA) on the DATC campus; specifically in the telecommunications closet. If there is sufficient network connectivity between the data center and the DBA, relocate

- salvaged data tapes/disks and equipment to telecommunications closets at the DBA and proceed to Restoring Systems.
- ii. Option 2: Cold Site Short Term
The cold site is located at the DATC's leased space at the Freeport Center in Clearfield, Utah. If systems cannot be restored at the DBA and if there is sufficient network connectivity between the data center and the Freeport Center, relocate salvaged data tapes/disks and equipment to the Freeport Center and proceed to Restoring Systems. Contact Utah Education Network and/or Qwest Communications to increase the bandwidth between Freeport Center Building A-15 to the data center. The T-1 currently in place may not be sufficient to handle all business communications.
- c. If the extent of damage to the data center and connectivity to telecommunications closets cannot be repaired within 14 days, choose one of the recovery sites for long-term system recovery:
 - i. Option 3: Warm Site Long Term
If there is no connectivity to the data center and repair is beyond 14 days then relocate salvaged data tapes/disks and equipment to the DBA and proceed to Restoring Systems. After systems are restored, relocate and establish other business resources to the DBA to perform essential business functions.
 - ii. Option 4: Cold Site Long Term
If there is no connectivity to the data center and repair is beyond 14 days and DBA is unusable then relocate salvaged data tapes/disks and equipment to the Freeport Center and proceed to Restoring Systems. After systems are restored, relocate and establish other business resources to the Freeport Center to perform essential business functions.

V. Restoring Systems

- a. Use salvageable equipment if possible. If equipment works but appears to have a short life span, consider replacing damaged yet working equipment as soon as possible.
- b. If equipment is damaged beyond repair, work with Procurement to expedite replacement equipment according to specifications in Appendix B.

VI. Network Infrastructure

- a. Data Center
 - i. Identify usability of core routing equipment
 - ii. Salvage usable equipment and restore functionality
 - iii. Order unsalvageable core routing equipment
 - iv. If data center is unusable, identify the usability of the Warm Site and make provisions to establish the data center at the warm site. If Warm Site is used then a high speed connection will need to be made from the Warm Site to the main campus.
 - v. If the data center and Warm Site are unusable, identify the usability of the Cold Site and make provisions to establish the data center at the Cold Site. If the Cold Site is used then a high speed connection will need to be made with a telecommunications vendor from the Cold Site to the main campus.

- b. Identify usability of network equipment in telecommunications closets
 - i. Identify usability of edge routing equipment
 - ii. Salvage usable equipment and restore functionality
 - iii. Order unsalvageable edge routing/switching equipment
- c. Identify usability communication lines
 - i. Identify usability of fiber optic, copper wiring, and other communication media
 - ii. Determine where the communication breakdown is located between the data center and telecommunication closets
 - iii. Attempt to fix breakdown and/or identify a vendor to repair breakdown

VII. Systems/Platforms Recovery

- a. File Servers
 - i. Identify usability of system/file server equipment
 - ii. Salvage usable system/equipment and restore functionality
 - iii. Order unsalvageable system/file server equipment
- b. Storage Area Network (SAN)
 - i. Identify usability of SAN equipment
 - ii. Salvage usable SAN and restore functionality
 - iii. Order unsalvageable SAN equipment
 - iv. Check connectivity to servers
- c. Backup/Restore Device(s)
 - i. Identify usability of backup/restore equipment
 - ii. Salvage usable backup/restore and restore functionality
 - iii. Order unsalvageable backup/restore equipment
 - iv. Check connectivity to file servers

VIII. Restore the Directory

- a. Locate backup media containing directory
- b. Restore directory from back media
- c. Test directory security objects by logging into system
- d. Ensure security objects restored properly and appropriate security credentials are in place
- e. Test other directory objects

IX. Mission Critical System Applications

- a. Locate backup media containing application(s) installed on server(s)
- b. If media is not accessible, locate installation disks and customized configuration (if any customization exists)
- c. Install application as outlined according to documentation

X. Restore Application Data

- a. Locate backup media containing applications
- b. Restore most recent full backup as recorded in backup log book
- c. Restore most recent differential backup as recorded in backup log book
- d. Verify applications is running properly on file server(s) once restored

XI. Client Access to Applications and Peripherals

- a. Restore access to applications and systems and ensure proper access to applications from client computers
- b. Restore access to printers ensure proper access to printers from client computers
- c. Restore access to scanners ensure proper access to scanning equipment from client computers

SECTION IV: Cyber Incident Response Plan

The Cyber Incident Response Plan establishes procedures to address cyber attacks against an organization's IT system(s). These procedures are designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial of service, or unauthorized changes to system hardware, software, or data (e.g. malicious login, such as a virus, worm, or Trojan horse).

Computer Crime

Computer crime is becoming more of a threat as systems become more complex and access is more highly distributed. Computer crime usually does not affect hardware in a destructive manner. It may be more concealed, and may often come from within.

Preventative Measures

Equipment such as firewalls and proxy servers has been installed to protect against unauthorized entry. All systems are protected by passwords, especially those permitting updates to data. All users are required to change their passwords on a regular basis. System users are regularly reminded the importance of keeping their passwords secret and reminded to choose strong passwords that are very difficult to guess.

All security systems should log invalid attempts to access data, and security administrators should review these logs on a regular basis.

All email will be scanned for virus laden attachments and a spam filter implemented to decrease the amount of unwanted email messages coming into and out of the DATC system.

All systems are backed up on a regular basis compliant with College policy. Tape/disk backups are stored in a fireproof lock box in the data center and off-site at the Freeport Center and are rotated on a regular basis as well. The data center is physically secure through issuing physical and electronic keys to limited personnel.

Computer Crime Recovery Procedures

- I. Assess the damage done by perpetrator and prevent perpetrator from further damage and/or exposure
- II. Assess College security risk and intrusion point
- III. Notify College President's Council of computer crime
- IV. Notify authorities of computer crime
- V. Rebuild/restore lost data

Appendix A: Vendor Contacts

Vendor Name	Contact	Web Information	Address
Cache Valley Electric	Phone: 435 752 6405 Fax: 435 752 9111	www.cve.com	919 North 1000 West Logan, Utah 84321
CDWG		www.cdwg.com	
Dell		www.dell.com	
Microsoft		www.microsoft.com	
Verizon Wireless	Larry Lewis	www.verizonwireless.com	
UEN	801.585.7440	www.uen.org	
NACR	Jodi Arave 801.726.0204	www.nacr.com	
Tenacious	Dana Johnson	www.gettenacious.com	
Salt Lake Valcom	Jamie Maxfield	www.slcv.com	
Qwest	Andrew Swensen	www.qwest.com	
Novell		www.novell.com	
Prime Systems	Josh Prince 801.546.2666		
Premier Computing	Andy Casper Rob Gillespie Main phone: 801-487-8400 Main fax: 801-487-8416 Service phone: 801-487-1001	www.premiercomputing.com	385 West 2880 South Salt Lake City Ut, 84115

Appendix B: Replacement Equipment