

Westminster College

Information Technology Department 2006-2007 Business Continuity and Disaster Recovery Plan

Summary

This document covers the following:

- Business continuity plan, including risk analysis, mitigation, preparedness, and practices; and
- Disaster recovery plan, including recovery team organization and critical systems prioritization.



Table of Contents

1.	Introduction	1
2.	Business Continuity Plan	1
2.1.	Risk Analysis.....	1
2.2.	Risk Mitigation.....	1
2.3.	Ongoing Preparedness	2
2.4.	Data Backup	2
2.4.1.	Backup Media Rotation.....	3
2.4.2.	Data Restoration Testing	3
2.5.	Data Archiving.....	3
2.6.	Network Equipment Management	3
2.7.	User Account Management	4
2.7.1.	New Faculty, Adjunct Professor, and Staff Accounts.....	4
2.7.2.	New Student Accounts	5
2.7.3.	Account Termination.....	5
2.8.	Password Management	5
2.9.	Software Management	5
3.	Disaster Recovery Plan	6
3.1.	Incidents Requiring Action.....	7
3.2.	Recovery Team Organization.....	7
3.2.1.	Recovery Coordinator.....	7
3.2.2.	Administrative & Network Computing Manager	7
3.2.3.	Computer Support & Web Manager.....	8
3.3.	Recovery Team Headquarters.....	8
3.4.	Critical Systems Prioritization	8
3.5.	Equipment Replacement	9
3.6.	Failure in the Central Machine Room	9
3.7.	Failure at Remote Areas.....	10

1. Introduction

Westminster College relies heavily on information technology services to support the college's mission and operation. A campus-wide network of distributed data, voice, and video components ties users to centralized resources. The importance of these systems to college operations requires a plan for ensuring that critical information technology services can be restored in a reasonable amount of time following service interruption.

This document is intended to address ongoing business continuity efforts and, in the event of an incident, recovery plans for information technology services. As such, it is a work in progress.

2. Business Continuity Plan

2.1. Risk Analysis

Westminster identifies the following broad categories as potential risks that can destroy or interrupt information technology services:

- Power interruption.
- Air conditioning or other environmental interruption.
- Fire.
- Water.
- Weather, earthquake, or other natural phenomenon.
- Sabotage or interdiction.
- Network security breach.

2.2. Risk Mitigation

Westminster has the following systems, policies, and practices in place to mitigate risk:

- The central Information Technology machine room is equipped with an HVAC temperature and humidity control system and a UPS that switches over to a generator in 30 seconds. The generator is tested each Friday afternoon, and it is refueled and maintained regularly by Plant Operations. Power conditioning and UPS services do not extend beyond the core of the computing center. The generator will run the machine room HVAC and equipment for 24 hours. A redundant HVAC system is in place and can be manually activated as needed. If the power outage is expected to last longer than 24 hours, Information Technology staff will initiate manual shutdown procedures. Upon loss of power, the Information Technology department will contact Plant Operations to ensure they are aware of the outage, as they have primary responsibility to communicate with the electric supplier and to update Information Technology with the best estimate of repair times.
- Office air temperature in the Giovale Library is controlled via an HVAC maintained by Plant Operations. In the event of air conditioning or environmental interruptions which do not pose a health threat or personnel safety risk, simple practices such as opening facility doors with staff acting as security, use of electrical fans, and use of space heaters may allow for temporary business operations. Prolonged interruptions will be dealt with by Plant Operations, and unsafe conditions will result in personnel evacuation, notification of local

fire/safety authorities and Campus Security, and initialization of the Disaster Recovery Plan.

- Fire alarms and sprinkler systems are located throughout the Giovale Library and are routinely tested by Campus Security.
- Water level sensors are installed in the central machine room subflooring and are routinely tested by Plant Operations.
- The Information Technology department is a secure facility located in the basement of Westminster's Giovale Library. The department is open to authorized staff during the hours of 8:00 AM and 6:00 PM weekdays. Access is restricted to Information Technology personnel on weekends, holidays and after regular hours. Information Technology staff have coded access cards. The machine room is further locked and secured with an alarm.
- For network security, Westminster utilizes a CISCO PIX firewall, performs analysis on flow data from CATS, and has a redundant data network. In the event of a suspected network security breach, Information Technology personnel responsible for systems administration will be alerted and initiate incident management.

2.3. Ongoing Preparedness

The following steps must be performed on an ongoing, regular basis to ensure Information Technology's preparedness for potential service interruptions:

- Maintain and update this plan.
- Maintain and update systems documentation, procedure manuals, and information.
- Ensure that all IT personnel are aware of proper emergency and evacuation procedures.
- Ensure that all IT personnel are aware of their responsibilities in the event of an incident.
- Ensure that data is being consistently backed up and can be reliably restored.
- Ensure that administrative system backup media is periodically rotated to off-site locations.
- Maintain a current status list of campus computing and network equipment.
- Ensure that emergency lighting and power systems are being routinely tested and are functioning properly.
- Ensure that fire and smoke detection systems are being routinely tested and are functioning properly.
- Ensure proper environmental standards are being met in equipment areas.
- Ensure that the user community is aware of the concept of disaster recovery, recovery procedures, and how an incident could affect normal operations.

2.4. Data Backup

For administrative system data backups, the Information Technology department uses an IBM DAT72 digital data storage tape drive.

For all other data backups, the Information Technology department uses BackUp Exec 10 software running on a Windows 2003 server connected to an ADIC Scalar 100 with two LTO1 drives. As of the time of this writing, we have requested an additional higher end ADIC with an LTO3 drive to further supplement our backup capacity and decrease backup time.

Data is backed up in the following manner:

- Administrative system data is backed up in full nightly, Monday through Friday. Data is kept for three months.
- User data is backed up in full every two weeks and incrementally three times per week. Data is kept for one month.
- Email is backed up in full three times per week. Data is kept for two weeks.
- Call manager phone databases are backed up in full three times weekly. Data is kept for one month.
- Voicemail is backed up manually once every three months. Voicemail data is moved to a location on the main network file servers and picked up during user data backups.
- Services such as system configurations, operating systems, website files, databases, directory services, etc. receive a full back up three times per week. Data is kept for two weeks.
- Local workstations are not backed up. All users are required to store data on backed up network storage locations.

2.4.1. Backup Media Rotation

Currently the Information Technology department has no formal policy on media rotation. Backup media is theoretically used until the media reports errors. Media reporting errors is assumed bad, destroyed, and replaced with new media. The Information Technology department is researching industry standards for media rotation and replacement and will adopt a methodology during 2006.

2.4.2. Data Restoration Testing

The Information Technology department recognizes the importance of performing routine data restoration tests. Currently the department is not testing data restoration because of two prohibiting factors stemming from resource constraints, namely:

1. Lack of a suitable test environment to restore data, meaning that any data restorations tests would necessarily overwrite live data, and;
2. Lack of an available time window for restoring test data, since the current system is near speed capacity to backup live data during available evening and weekend hours.

2.5. Data Archiving

Data is archived in the following manner:

- Media backups of the Administrative databases are sent once per week to an off campus site for three months storage.
- Other data is not archived. Media backups are maintained on-site in the IT department in a secure, climate-controlled room.

2.6. Network Equipment Management

The college meets the following standards of physical security for the campus local area network:

- Premises housing network control equipment are physically strong and free from unacceptable risk from flooding, vibration, dust, etc.
- Internal building distribution of cables within ceilings, walls, and floor cavities are reticulated within protective conduits.
- Air temperature and humidity are controlled to within equipment defined limits.
- Essential network electronics are powered via un-interruptible power supplies to provide a minimum of 15 minutes operation in the event power loss and adequate protection from power surges and lapses.

2.7. User Account Management

Unique computer user accounts are created for all faculty, staff, and students. Additional departmental accounts are created specifically to centralize departmental email correspondence. Workstudy accounts are created to allow student employees limited access to shared departmental network folders. Graduates of the college may request one-year alumni computer account extensions from their date of graduation through the Alumni Relations office.

2.7.1. New Faculty, Adjunct Professor, and Staff Accounts

New faculty, adjunct professor, and staff computer accounts are created as follows:

1. A staff member from the Westminster Human Resources office completes and submits a secure online form. The form sends a secure email to an Information Technology staff member responsible for account creation. The form includes the following data:
 - First name
 - Middle initial (optional)
 - Last name
 - 7-digit Westminster ID number
 - Title
 - Department
 - Supervisor
 - Start date
 - Account type
 - Name of employee who previously held position (optional)
 - Additional information (optional)
2. The Information Technology staff member creates the computer user account, looking up necessary sensitive information through the college's administrative database. The account's access level is scoped to the position.
3. Upon creation of the account, the request email is deleted.
4. The new employee is required to meet with the Faculty Technology Center staff for an orientation session on campus computing systems and services. At that time, they are orally given their username and told the convention for their initial password (social security number). The employee is required to log in to a campus computer, and their password is

immediately expired. They are forced to change their password under the guidelines from the Information Technology Security Policy.

2.7.2. New Student Accounts

Student accounts are created as follows:

1. Following registration deadlines, student accounts are created by batch process directly from the college's administrative database.
2. All new students are required to attend a Computer Orientation session led by Information Technology staff. During the orientation students are told the convention for their username and password. They log in and immediately change their passwords. Students unable to attend an orientation may receive one at any time from the General Computing Lab staff.

2.7.3. Account Termination

User accounts are terminated as follows:

The computer user accounts of persons leaving the college or no longer requiring access are disabled upon notice from HR for employees leaving the college and from the appropriate custodian of the application for employees no longer requiring access. Student user ids are disabled for unregistered students the second week of fall and spring semesters. All files are referred to the system custodian for disposal.

2.8. Password Management

Passwords are managed under the following policies:

- For faculty, adjunct professor, and staff computer user accounts, automatic password aging is enforced on network systems. The life of a password is 120 days.
- For student accounts, passwords do not expire. Students are required to change their password upon first login.
- Passwords are encrypted and administrative system passwords are shadowed.
- On the administrative system, failed login forces a delay. After nine failed tries, the account is deactivated and the system administrator must be contacted for account reactivation.
- The current password convention is a minimum of 5 characters. However, users are regularly educated about password guidelines as defined in the Information Technology Security Policy. Users are instructed to use longer, non-dictionary alphanumeric passwords with mixed case.

2.9. Software Management

The Information Technology department manages all aspects of critical campus software including operating systems, associated packages and utilities, and third party and college-developed applications together with any command procedures and documentation to support and run them.

When changes are required to critical systems software, associated packages and utilities, applications software, command procedures, or documentation, the changes must be:

- Appropriately authorized and approved.
- Thoroughly tested.
- Sufficiently documented.
- Implemented at an appropriate time.

Where possible, three separate environments are maintained for each critical software system:

- Development environment;
- Testing environment; and
- Production environment.

New software and changes to existing software are prepared in the development environment by appropriately authorized development or applications support staff. Once assessed as satisfactory, the new or modified software should be transferred to the testing environment for systems and acceptance testing by an appropriate testing group.

Following successful completion of testing and approval by the appropriate systems custodian, the new or modified software is transferred to the production environment for implementation. A contingency plan is prepared where appropriate to enable the software to be restored to its previous version in the event that the implementation is unsuccessful.

3. Disaster Recovery Plan

The disaster recovery plan contains general operational assumptions but does not attempt to consider all situations that can occur. Decisions for situations not covered in the plan will be made, as required, by the senior Information Technology staff member on-site.

The senior Information Technology staff member on-site at the time of the incident will assume immediate responsibility. The first responsibility will be to see that, if necessary, people are evacuated to a safe area. If injuries have resulted, immediate attention will be given to those injured persons. Campus Security and the Plant Operations will be notified, if necessary. If the situation allows, attention will be given to shutting down systems, turning off power, and securing data, but evacuation to a safe area is the highest priority.

The senior staff member available at the time of occurrence, or the first on-site following a potential incident, will contact the Director of Information Technology, the Administrative & Network Computing Manager, and the Computer Support & Web Manager with regard to the need to declare an incident. Once an incident has been declared, the plan will remain in effect until emergency response authorities have been notified, if appropriate, and the incident is substantially resolved. Invoking the plan implies that a recovery operation has begun and will continue with the highest priority until such time as essential systems under control of Information Technology have been restored.

The variable degree of incident severity necessitates different strategies for partial and full systems recovery, defined as:

- Partial recovery: operating at a) the current central site, or b) an alternate location on campus, or c) an off-campus location, with some critical systems running but likely at a degraded level of service, for a period of time.
- Full recovery: operating at the current central site and user areas, with most critical systems

running, for a period of time.

3.1. Incidents Requiring Action

This plan will be invoked under one of the following conditions, or at the discretion of the Director of Information Technology:

- An incident has disabled, or is expected to disable, the central computing facilities and/or the communications network to the degree that normal operations will be significantly impacted for a period of 24 hours or more.
- An occurrence beyond the scope of daily operations has impaired the use of computers, telephone, or communication facilities in a manner that will substantially impact the normal operation of the college.
- An accident caused by problems with computers, communications systems, or equipment managed by Information Technology has resulted in the injury of one or more persons.

3.2. Recovery Team Organization

In the event of a declared incident, the Recovery Team will be assembled. The team will be led by the Recovery Coordinator who will in turn direct two team leaders: the Administrative & Network Computing Manager and the Computer Support & Web Manager. Remaining Information Technology staff will be assigned into subordinate teams.

The subordinate Recovery Team structure will default to current reporting lines. However, the need for flexibility during an emergency is paramount and staff members will be organized into teams as needed. Team structure will necessarily be dependent upon the types of expertise required by the particular incident, and staff will be assigned to tasks during recovery by the team leader responsible for that area, as directed by the Recovery Coordinator.

3.2.1. Recovery Coordinator

The Director of Information Technology will serve as Recovery Coordinator and will:

- Invoke the Information Technology disaster recovery plan.
- Determine the extent and seriousness of the incident, notifying the Provost and Executive Vice President and keeping them updated on the status of the recovery effort.
- Locate any Recovery Team members that are not on-site and request their return, then name replacements for any unavailable Recovery Team members.
- Coordinate priorities for partial recovery of user systems and move toward full recovery.
- Supervise the recovery activities.

3.2.2. Administrative & Network Computing Manager

The Administrative & Network Computing Manager will:

- Evaluate and provide recommendations for restoring IT facilities systems and operational software, as well as software critical to network operations.
- Supervise and coordinate hardware replacement activities with appropriate hardware vendors.

- Supervise recovery of backup media from off-site storage and institute recovery procedures.
- Coordinate recovery activities with the Computer Support & Web Manager and other IT staff.
- Coordinate interim system production schedules and other centralized user services.
- Keep the Incident Recovery Coordinator and other team members informed of the status of recovery procedures being implemented.

3.2.3. Computer Support & Web Manager

The Computer Support & Web Manager will:

- Evaluate and provide recommendations for restoring website systems.
- Implement and update emergency messaging on the college home page, if needed.
- Coordinate website systems recovery activities with external systems suppliers and third-party vendors.
- Coordinate end-user support in the event of the need to use alternative access methods or alternative products to provide interim user services.
- Coordinate recovery activities with individual user departments.
- Act as the primary point-of-contact for the Office of Communications and individual users.
- Keep the Incident Recovery Coordinator and other team members informed of the status of recovery procedures being implemented.
- Communicate to users the status of campus network services.

3.3. Recovery Team Headquarters

The recovery team will use the following guidelines to establish team headquarters:

- If the downstairs Giovale Library is usable, the Recovery Team will convene in the IT department offices.
- If the downstairs Giovale Library is unusable, the Recovery Team will convene in the Nightingale Hall foyer.
- If the Nightingale Hall foyer is unusable, the Incident Recovery Coordinator will locate an appropriate on-campus location.
- If on-campus facilities are unavailable, the Incident Recovery Coordinator will make appropriate arrangements in concert with the college's senior administration in accordance with the college-wide Disaster Recovery Plan.

3.4. Critical Systems Prioritization

The following systems are considered critical to supporting the college's business operations and communications needs. The Recovery Coordinator will prioritize efforts to restore critical systems. Establishment of basic communications capabilities will be the highest priority in the event of the loss of multiple critical systems, followed by essential data processing functions, networking, wide-area network capabilities, and lastly, complete networked data services to user workstations.

The default priority for system restoration will be as follows, with adjustments made by the Recovery Coordinator as necessary:

Primary:

- Core network services.
- Phones.
- Web site message page.

Secondary:

- Administrative database.
- Email.
- Printing.

Tertiary:

- Computer and presentation classroom equipment.
- Support phone and user support services.

3.5. Equipment Replacement

All college equipment is covered against loss by college insurance policies. In a declared emergency, equipment may be obtained by phone or fax bid, bypassing normal college bid procedures. The central computing facility uses HP, Cisco, IBM, and Intel-architecture equipment, which is typically available from either the manufacturer or equipment suppliers and can be obtained within a 24-72 hour time span. Westminster has a maintenance agreement with IBM which specifies that the vendor guarantees a 24-hour replacement window for hardware failures on key systems.

Network equipment can be supplied by Cache Valley Electric, Cisco and various resellers from stock. Network systems are based on Intel-architecture PCs and can be replicated from spares, stock, and parts from local suppliers within reasonable timelines.

3.6. Failure in the Central Machine Room

This portion of the plan will be activated when an incident has occurred that requires use of a location other than the IT department, or damage to the central machine room is such that operations can be restored, but only in a severely degraded mode.

In the event of an incident disabling central machine room operations, the Recovery Coordinator will oversee the following steps:

- Determine the extent of damage, the operational level of salvageable equipment, and if additional equipment and supplies are needed.
- Assign personnel to teams. The Recovery Coordinator will develop priorities after an evaluation of the extent of damage following the incident.
- Determine whether the central site may be used to restore service or whether an alternate location must be activated. If an alternative site is required, inform college officials that an alternative site will be necessary to continue operation.
- Obtain approval for expenditure of funds to bring in any needed equipment, supplies, or

additional expertise.

- Notify vendor marketing and/or service representatives if there is a need of immediate delivery of components to bring the systems to an operational level, even in a degraded mode. Obtain information from additional vendors and suppliers to see if faster delivery can be obtained.
- Notify vendor support personnel that assistance is needed, involving them at the earliest opportunity of the restoration process.
- Review need for equipment or parts not normally considered part of a replacement equipment order, such as electrical cables, fibre patch panels and cables, copper connectors, etc.
- Rush order any forms, supplies, or media needed.
- If using an alternative location, coordinate moving equipment and support personnel into the alternate location.
- As soon as basic equipment is (re)assembled, load operating systems, operational software, load most current backups, and commence testing and certification procedures.
- Determine need to supply connectivity to work-around areas that are inaccessible or have been destroyed. Place emergency orders for any materials needed to accomplish necessary splicing, testing and certification of network and communications systems.
- If appropriate, set up lab environment for continuance of critical services until such time as communications infrastructure can be restored.
- Determine priorities of user operations, and load any special systems in order of most critical need.
- Prepare backup materials and return to safe storage.
- Reactivate user support services.
- Commence critical operations, resuming production and backup procedures as facility capacity is grown to requirements.
- Create a schedule to ensure that all critical support services are phased in.
- Keep administration and users informed of status, progress, and problems.
- Coordinate long range plans for full restoration of services.

3.7. Failure at Remote Areas

Remote areas supply a far smaller group of people than does the central site, thus many of the functions needed by these users can be replicated in alternate areas of the campus during the course of a declared incident. The amount of downtime tolerated in any area will be determined by the senior administration in concert with the Recovery Coordinator, and recovery procedures will be modified dependant upon the nature and extent of the incident.

No efforts will be made to recover workstation data. Workstation hard drives are not backed up and users are required to save all data to the network. If workstation software is corrupted, the workstation will be loaded with a fresh image of college approved software. Workstation hardware will be replaced as needed.