CAPE COD COMMUNITY COLLEGE

Powerful Futures Start Here

# Cape Cod Community College

Emergency Procedures

&

Disaster Recovery Plan

Table of Contents

## 1.0 Emergency Procedures - General

It is impossible to plan for all emergency situations. However, it is possible to react in a manner that will prevent an emergency from becoming a disaster.

In an emergency:

**Evaluate the Situation**

Quickly evaluate the situation to determine what steps should be taken.

**Use Common Sense**

Do not try to save the computer equipment or software if it means risking your life. It is more important to get out of the building and notify the proper authorities.

## 1.1 Telephone Numbers

| | |
|---|---|
| Fire, Police, Ambulance, Off Campus Emergencies | 911 |
| Department of Public Safety (Facilities after hours) | 4349 |
| Facilities 8:30-4:30 | 4177 |

## 1.2 Emergency Equipment Locations

### Password List:

Cape Cod Community College uses "Passpack" online password management database service (http://www.passpack.com/online/#0) Directors records their system passwords on Passpack and transfer the ownership to Network Administrator/ISO. A list with Passpack website login account and the other system passwords, key code information, safe combinations, etc., is in the fire safe in the Human Resources safe. Only the HR personnel have an access to the safe. A second password list is located in the fire safe in the CIOs Office.

The following IT staff has the combination to this safe:

Chief Information and Technology Officer (CITO)
Director of Network and Client Services

### Uninterruptible Power Supply:

One to two UPSs will be located in each rack to power servers and switches in that rack. Periodic review of and testing should be performed. Batteries and/or devices should be replaced whenever they become faulty.

### Breaker Boxes:

There are two breaker boxes in the Lorusso NOC. One is for generator and one for non-generator powered circuits inside the room. In the Library, there are two breaker boxes located just outside of the loading dock. These control all the power for the Library NOC. There is a breaker box for the NOC only behind the racks.

## Fire Alarm Pull Switch:

The Fire Alarm for the Lorusso NOC is in the hallway outside the Work Room. Fire Alarms for the Library are located by all exterior exit doors throughout the building.

## Fire Extinguisher:

A fire extinguisher is located inside the Lorusso NOC and in the corner outside of the Library NOC. These extinguishers are Halon. Halon fire extinguishing systems use a halogenated hydrocarbon as a fire-extinguishing agent. The Halon agent inhibits the chemical reaction of fuel and oxygen, thus stopping the combustion chain reaction. Halon is non-corrosive and does not damage sensitive equipment.

Fire extinguishers can save lives and property by extinguishing a small fire or containing it until the Fire Department arrives. Fire extinguishers are not designed to fight large or spreading fires. The following guidelines apply when using a fire extinguisher:

Activate a fire alarm prior to using a fire extinguisher.
Always position yourself with an exit before use.
Do not use the extinguisher if there is a large amount of smoke.

The easiest way to remember how to fight a fire with a fire extinguisher is to remember the acronym, PASS, which stands for Pull, Aim, Squeeze, and Sweep.

PULL the pin at the top of the extinguisher.
AIM the extinguisher nozzle toward the base of the fire while 6-8 feet away.
SQUEEZE the handle to discharge the extinguisher.
SWEEP from side to side

## 2.0 Emergency Procedures - Fire

### 2.1 Paper Fire in the Lorusso NOC

Pull fire alarm switch in the hallway.
Call 911.
If possible without personal danger, use fire extinguisher to contain fire.
If possible without personal danger, turn air conditioners off using the two thermostats located on either side of the Lorusso NOC.
If possible without personal danger, shut down computer equipment in the Lorusso NOC.

### 2.2 Paper Fire in the Library NOC

Pull fire alarm switch next to loading dock doors.
Call 911.
If possible without personal danger, use fire extinguisher to contain fire.
If possible without personal danger, turn air conditioners off using the two thermostats located in the rear of the Library NOC.
If possible without personal danger, shut down computer equipment in the Lorusso NOC.

### 2.3 Electrical Fire in Lorusso NOC

Pull fire alarm switch in the hallway.
Call 911.
If possible without personal danger, turn off the UPSs to the equipment. Cut off power at the breaker boxes on the wall if necessary.
If possible without personal danger, use fire extinguisher to contain fire.
If possible without personal danger, turn air conditioners off using the two thermostats located on either side of the Lorusso NOC.

### 2.4 Electrical Fire in Library NOC

Pull fire alarm switch next to the loading dock doors.
Call 911.
If possible without personal danger, shut off power by turning off the UPS's to the equipment. Cut off power at the breaker box behind the left rack.
If possible without personal danger, use fire extinguisher to contain fire.
If possible without personal danger, turn air conditioners off using the two thermostats located in the rear Library NOC.

## 3.0 Emergency Procedures – Water Leak

In the event of a sprinkler activation or water leak in the ceiling of either the Lorusso or Library NOCs steps must be taken to mitigate damage.

## 3.1 Water leak in the Lorusso NOC

Contact Facilities at 4177
Call 4349 or 911.
If possible without personal danger, turn power off to affected equipment UPSs or at the breaker boxes.
If possible without personal danger, throw tarps that are under the desk over the racks to prevent water from getting on the equipment.

## 3.2 Water leak in the Library NOC

Contact Facilities at 4177
Call 4349 or 911.
If possible without personal danger, turn power off to affected equipment UPSs or at the breaker boxes.
If possible without personal danger, throw tarps that are under the desk over the racks to prevent water from getting on the equipment.

## 4.0 Emergency Procedures – Power Outage

In the event of a power outage, the UPS's in the NOCs will start backup power immediately. They will begin counting down how much time is remaining of backup power. The UPS's will power all equipment on the floor in the NOCs.

There is generator power only to select equipment in the Lorusso Building NOC. One air conditioner in the Lorusso NOC is powered by generator. There is no generator power to equipment in the Library NOC.
Whenever a power outage occurs take the following action:
The Director of Network and Client Services will take the lead and decide what action to take in response to the power outage in the NOCs. Contact the Director of Network and Client Services immediately:

The Director of Network and Client Services will consult with the Systems Development Director and Client Services Manager to determine what additional action or assistance might be required. The Director of Network and Client Services will direct action to limit potential damage to equipment. These actions may include:

- Shut down servers and other equipment in the NOCs
- Power off all non-essential equipment (printers, tape drives, etc) to save power for critical systems.
- Call to find out the status of the power: Facilities or Public Safety
- Keeping the CITO informed of the situation.

When normal power is restored, the Director of Network and Client Services will direct action to restore services as quickly as possible.

## 4.1 Emergency Procedures - Air Conditioner Failure

### Computer Room Temperature

The Lorusso NOC is air conditioned by two three-ton air conditioning units. The Library NOC is air conditioned by a single five-ton air conditioning unit.
If the NOC air conditioning performance drops to a level that is unacceptable Network Administrator should be notified. The Network Administrator will assess the situation and will notify the Director of Network and Client Services if needed.
If the temperature in either NOC reaches 90 degrees and there is no indication the air conditioning will soon be restored non-essential equipment should be shut down.
If the temperature in either NOC reaches 95 degrees, all equipment will be shut down until air conditioning is restored to prevent damage to equipment.

## 5.0 Emergency Procedures - Unauthorized Entry to Computer Room

If an unauthorized individual enters either NOC area and refuses to leave or the activities of the unauthorized person are suspicious:

Call Public Safety 4349.
Try to keep the individual out of the NOC but avoid provoking the intruder.

If evidence is discovered an unauthorized access to the NOC area has occurred the following action should be taken:

Call the CITO or Director of Network and Client Services in the CITO's absense .
Call Public Safety 4349.

## 6.0 Disaster Recovery Plan

There are several different types of "disasters" that can affect technology services. These range from hardware failures that result in the loss of data to major disasters such as fire, flood or hurricanes. It is impossible to develop a detailed plan that covers every known emergency. Rather, it is important to develop a framework or outline to provide guidance in the event of a disaster. Key personnel must be aware of the resources and options available and be prepared to develop a plan to meet the specific crisis at hand.

## 6.1 Prevention and Preparedness

Prevention of inadvertent or malicious damage to technology systems and services is the first layer of defense. Maintenance of a safe and secure environment is critical. However, prevention is not always successful; therefore, backup systems and alternative paths and locations for restoring services must always be considered.

### A) Physical Security

Physical Security is the first line of defense against unauthorized system access. All critical network, administrative, and academic systems are housed in the NOCs. These rooms have single-entry points controlled by a key-pad/magnetic lock. Only appropriate personnel are authorized entry.

### B) Network Systems

The network is the physical infrastructure that carries voice, data, and video traffic on campus and connects that traffic to the outside world. The network consists of:

- Cable infrastructure - optical fiber, copper, and connecting devices.
- Hardware components - hubs, routers, switches, cameras etc.
- Servers - computers of various makes running the Windows Server operating system.

The fiber optic infrastructure has a large amount of spare capacity which can be used should damage or failure affect a portion. A large amount of the infrastructure is underground, protecting it from hazards such as lightning and falling trees. The most likely catastrophic failure is the severing of an entire underground cable. In this case, alternative paths should be evaluated by rerouting traffic or possibly by substituting old 62.5 micron fiber for 50 micron fiber that is used by the current network.

### C) Telephone System

The Cape Cod Community College telephone system is a cloud-based, VoIP service currently contracted through 8x8, providing ringtone and voicemail. The system runs on our data network and utilizes our Internet connections for calling. In the event that our data network is disrupted, phone services will also be disrupted.

### D) Data Assurance

Cape Cod Community College uses an HP Nimble storage area networks (SAN). The production SAN is located in the Lorusso NOC.

### E) Data Backup

A major concern in a disaster is the protection of data. Back-ups are performed nightly. Physical Servers and Virtual Servers are backed up to disk as well as to a cloud-based data backup service contracted through a company called Wasabi.

### F) Severe Damage to a NOC

In the event of severe damage to one of the NOCs the IT Department leadership will evaluate the situation and consider switching operations to the alternative NOC and moving undamaged equipment in an effort to restore services as quickly as possible. If equipment is damaged and cannot be moved the IT Department leadership will immediately begin an assessment of prioritized need for replacement equipment to be acquired and data restored from backup.

### G) Hurricanes

Hurricane season starts June 1 and ends November 30. Cape Cod is highly vulnerable to hurricanes. Hurricanes that impact Cape Cod track through or originate in the Bermuda area. These storms move quickly and can arrive on shore only 24 hours after formation.

The speed of these hurricanes reduces reaction time and increases the power because the speed of advance is added to the hurricane wind speed to get the true velocity. Because reaction time is so limited in the event of a hurricane decision-making must be quick and effective.

When a tropical storm warning or hurricane watch is posted for Cape Cod the IT Department staff will begin preparations to protect equipment and ensure vital services are provided as long as is possible.

The Hurricane Preparedness Plan will be consulted for guidance.

Upon direction to implement the Disaster Recovery Plan in the event of a hurricane the following procedures will be followed:

## 6.2 Disaster Recovery Actions Related to Alternative Hosting

| | |
|---|---|
| Phase 1<br><br>Within 4 hours of decision to implement Disaster Recovery Plan | Assemble Office of Information Technology Disaster Recovery Team in the Lorusso Building or alternate site.<br>CITO notify designated hosting site of potential deployment of DR equipment to host.<br>Client Services Manager secure transportation vehicle.<br>Director of Network and Client Services and Systems Development Director begin preparation of servers and associated DR equipment for transport to designated host site. |
| Phase 2<br><br>Within 8 hours of activation | Disassemble DR equipment for transport and load on truck.<br>Seek President or VP A&F permission to move equipment.<br>Notify designated host site of decision to move DR equipment |
| Phase 3<br><br>Within 12 hours of activation | DR equipment arrives at designated host site.<br>DR equipment is unloaded.<br>Conduct assessment of needs at host site.<br>Contact SAN Vendor and notify of potential need for assistance at designated host site. |
| Phase 4<br><br>Within 24 hours of activation | DR equipment ready for activation at designated host site.<br>Re-assess situation in consultation with President and/or VP F&A regarding disaster at main campus. Decision to Hold or continue preparations for DR activation at designated host site.<br>If Re-assess damages at affected site and determine if return is feasible. If not, establish more-permanent recovery site. |
| Phase 5<br><br>Dependent on many factors | Return to primary site or convert DNS and activate DR systems. |

| Support Personnel List for Disaster Recovery | | | |
|---|---|---|---|
| Name | Title | Expertise | Phone |
| Richard Wixsom | CITO | DR | 774-330-4701<br>508-367-9884 (cell) |
| Chuck Phelan | Director of Network and Client Services | Servers | 774-330-4707<br>508-367-9897 (cell) |
| Eric Sheffer | Systems Dev Dir | Data/Apps | 774-330-4702<br>508-367-8530 (cell) |
| Konur Oz | Client Services Manager | Network | 774-330-4413<br>508-367-9891 (cell) |

**Appendix A:**

Information Technology Staff Directory

| Name | Title | Extension | Cell Phone | Personal Phone | Email |
|---|---|---|---|---|---|
| Richard Wixsom | CITO | 4701 | 508-367-4772 | 413-281-4346 | rwixsom@capecod.edu |
| Chuck Phelan | Dir. of Network & Client Services | 4707 | 508-367-9897 | 508-420-1993 | cphelan@capecod.edu |
| Eric Sheffer | Dir. of Systems Development | 4715 | 508-221-2268 | 508-385-8393 | esheffer@capecod.edu |
| Konur Oz | Client Services Manager | 4413 | 508-367-9891 | 508-744-7008 | koz@capecod.edu |
| Dona Alexander | Business Analyst | | | | dalexander@capecod.edu |
| Doug MacKenzie | Systems Developer | 4997 | | 508-945-3041 | dmackenzie@capecod.edu |
| Jerry Schmeer | Programmer III | 4601 | 508-280-0192 | 508-444-0410 | jschmeer@capecod.edu |
| Chris Brisee | Web Master | | | | |
| Tim Garneau | Systems Analyst III | 4447 | 508-367-9895 | 774-994-0288 | tgarneau@capecod.edu |
| Scott Smith | Systems Analyst I | 4996 | 508-367-9815 | 5083859356 | ssmith01@capecod.edu |
| Erik Phillips | Systems Analyst I | 4704 | 508-3648961 | 508-521- | ephilips@capecod.edu |
| Ritchie Kolnos | Technical Specialist II | | | | rkolnos@capecod.edu |
| Chris Griffin | Technical Specialist II | | | | cgriffin@capecod.edu |
| Hok Woo | A/V Technician II | | | | hwoo@capecod.edu |
| | | | | | |

**Appendix B:**

Important Vendors and Contacts

| Vendor | Contact | Address | Phone | Fax | Tech Support | Email/web |
|---|---|---|---|---|---|---|
| Altiris | | PO Box 201584<br>Dallas, TX 75320 | 801-226-8500 | 801-226-8506 | 888-252-5551 | support@altiris.com |
| COMCAST | Business Services | | 888-737-8361 | n/a | 888-737-8361 | www.comcast-ne.com/business/contact.html |
| Dell Technical Support | | | 877-671-3355 | | 877-671-3355 | http://Support.dell.com |
| Open Cape | Steve Smith | | 508-856-4216 | | | |
| HPE | | | 800-633-3600 | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |