

# The University of the West Indies

## Disaster Preparedness Practices – The Mona Campus

Preparation for disaster includes:

- ✓ Physical preparation of the locations
- ✓ Redundancy provision for disaster mitigation
- ✓ Rules for powering down in preparation of the onset and powering up after the disaster

### Physical preparedness

The physical locations which are listed below address our main technology control points:

- The Data Centre at MITS (or MER1)
- MER2 which is in the vicinity of the Senate Building
- MER3 in the vicinity of Chemistry Department
- MER4 in the vicinity of Management Studies
- MER5 in the vicinity of the Assembly Hall
- MER6 in the vicinity of the Medical Library

MER stands for Major Equipment Room.

Our preparedness checklist for these physical locations:

Locations are prepared :	Critical actions
Backup electrical power supply is in place at each location	Service the generators - check for fuel and oil
Hurricane shutters have been installed in the appropriate building / area	Maintenance to put up the shutters at the start of the Hurricane season. <i>Note : the shutters are usually put up as soon as the first tropical disturbance threatens our geographical area.</i>
Data centre has fire detection system	
<i>We do not yet have fire suppression system</i>	
Three of the MERs also have fire detection systems (MER2, MER3, MER5)	
The selection of fire suppression system is in progress (but near term acquisition is not	

a certainty due to budget issues)

Structured cabling standards are adhered to the all buildings. [Cabling standards: ANSI/TIA/EIA 568-B \(US\)\]](#)

Electronic Access control is to be introduced soon to the Data Centre

### **Preparedness regarding enterprise data:**

There is a well understood, documented backup strategy for all enterprise data.

Enterprise data is backed up regularly on a daily, weekly, monthly basis. See related documents.

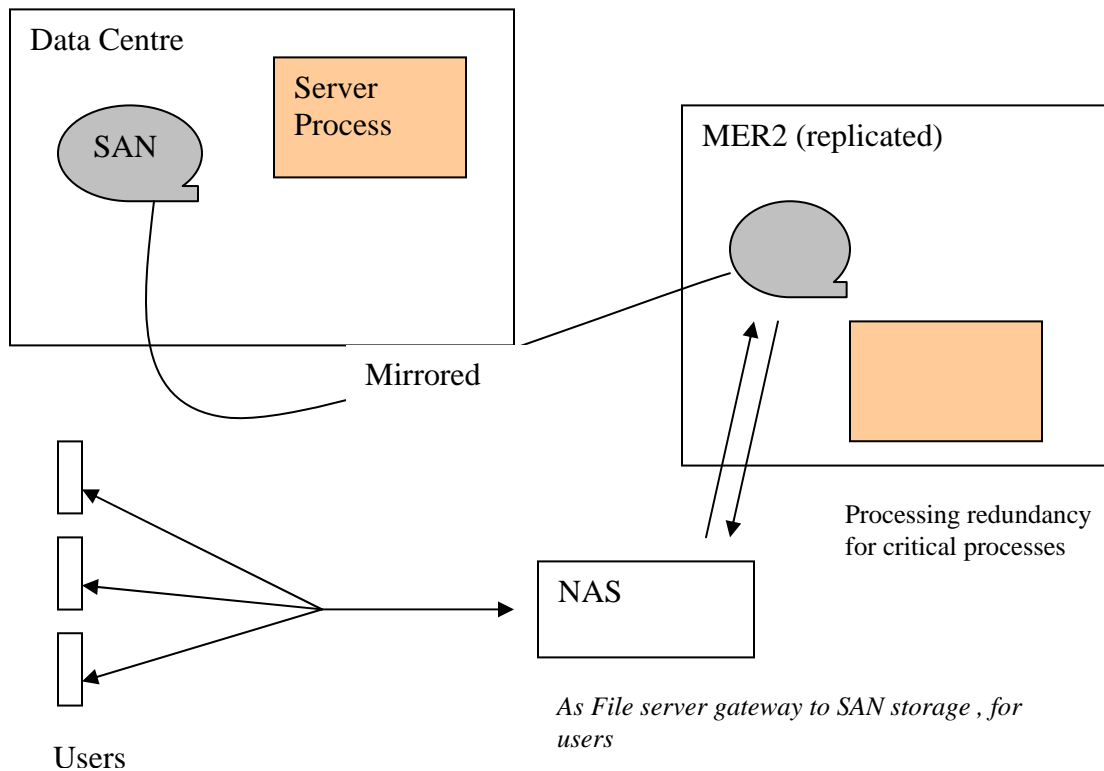
A copy of the backup is taken off site where it is stored in a bank vault, and another is placed in the MITS cabinet for backup tapes.

Note: the Campus needs to acquire a Safe which is water and fire proof  
Related documents titled:

- ✓ *BACKUP PROCEDURE SUMMARIED – TMA , Banner Finance and VTLS –The Library system*
- ✓ *Tape Rotation strategy*
- ✓ *STUDENT RECORDS SYSTEM BACKUP AND RECOVERY PROCEDURES*
- ✓ *Peoplesoft Backup and Recovery Procedures*

## System redundancy

The purpose is to establish a secondary Data Centre to act as a 'hot standby' for critical processes in the event of a disaster or stoppage of any kind. Such a centre is located at MER2.



*Note that the above strategy is not fully in place. The SANs are mirrored and the MER facility can activate seamlessly if the Data Centre SAN goes down. NAS is part of the current plan for the way forward.*

[\[Currently implementing server processing at secondary data centre site.\]](#)

## Internet Redundancy

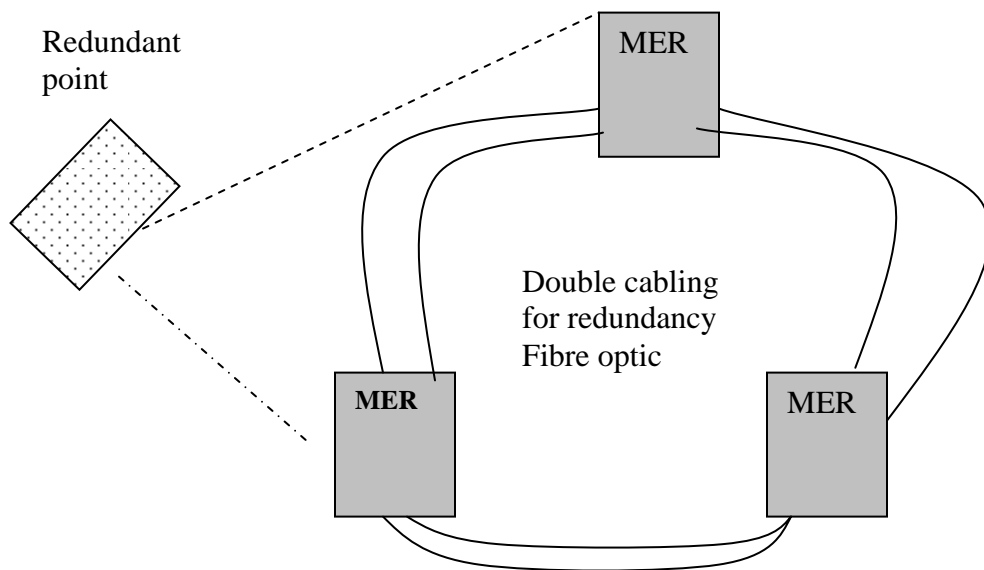
Redundancy is built into the Internet connectivity by having two links

- five (5) ADSL coupled to give approximately 10MB band width
- a direct 10MB broad band link

## Network Cabling Redundancy

Locations are connected by two cabling channels having a separation of about 5 feet. Whereas this is adequate protection in most cases it may not be sufficient to protect against a back hoe accident. The upgraded strategy is to create redundant cabling points.

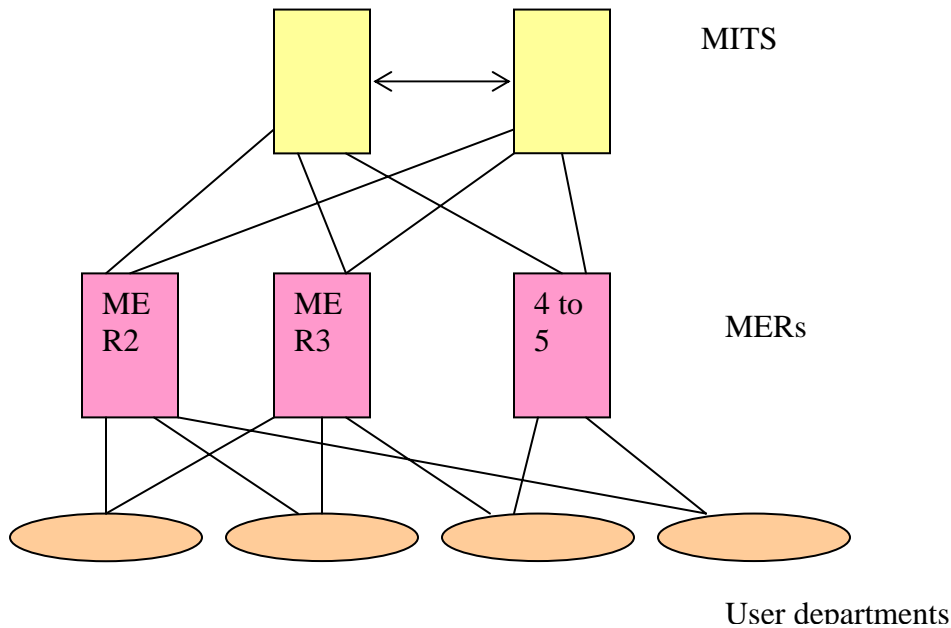
### Illustration



**Data redundancy** – is accounted for in the data backup and storage of backup tapes.

### **Connectivity redundancy**

The strategy is to ensure that all major connections are replicated. The diagram below illustrates the concept in place.



### Server redundancy

Our database servers, hosting our Oracle databases for our enterprise systems, are sufficiently similarly configured to allow mobility between machines. [\[Proposed acquisition of additional database server for increased capacity and redundancy\]](#)

### Rules /checks for powering down

- ✓ The decision to powering down in the event of a natural disaster is triggered by Civil Authority (ie the appropriate Government Agency). Secondly the communiqué issued by Campus disaster management team (Safety and Emergency Management Committee) informs the preparation activities by the advice or instructions given, for instance notice of closure.
- ✓ Hurricane Shutters would have already been placed in position. However, if not, then activate them at this point.
- ✓ Activate quick inspection and servicing of generator – check fuel and oil levels
- ✓ Check electrical panels to ensure that changeover switch is working. This is visual inspection.
- ✓ Take an incremental backup of all enterprise systems before powering down
- ✓ Safeguard in-house backup tapes (*we do not have fireproof waterproof safe*) as well as possible. Ensure that duplicates are sent off site

- ✓ Stay attentive to the broadcasts (internal and external) especially in order to find out if and when the Campus will be closed.
- ✓ Aim to shut down IT infrastructure two to three hours after stated time for closure.
- ✓ Determine if there are any critical processes to be run or are running, and facilitate them as far as possible.
- ✓ Shutdown the system from the outside in, thus starting at the periphery systems ie the departments, and working inwards to the MERs, then the backbone switches and finally the Data Centre. These switches are to be physically unplugged.
- ✓ At the Data centre the enterprise business applications are the last to be shut down.
- ✓ As far as possible MITS will attempt to keep core communication services running, in particular the Internet. These services are taken down only if there is direct threat to that particular facility or equipment. In such a case it is shut down remotely.

### **Precautions in bringing the ICT service back up**

Each physical MER location must be visited to ensure that no water damage or downed cables pose a threat to the location and its equipment. If the campus power supply has been significantly compromised (or seemingly so) an inspection from Maintenance is required before the equipment is switched back on.

All Systems Engineers and many of our experienced LAN administrators are aware of the rules and checks.