# uMtshezi Local Municipality
# IT Disaster Recovery Plan

## Document & Record Control



| | |
|---|---|
| Rohann Neethling<br>**Compiled By** | **Date** |
| Robert Edwards (IT Manager)<br>**Recommended By** | **Date** |
| **Authorised by** | **Date** |

Approved and Adopted by Council resolution no: **493.03.13**
Date: **26 March 2013**

## Amendment Record

| Rev | Section Affected / Reference | Date |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

## 1. Purpose

1.1 The purpose of the IT Disaster Recovery Plan is to ensure that, should the municipality experience disaster of any nature (e.g. firebreak, power surge or damage to the building, etc.), the municipality has contingency plans for backup systems.

1.2 The plan is there to make staff aware of what procedures should be followed when connecting backup systems and who the key contact persons for the systems are.

1.3 This Disaster Recovery Plan is there to ensure that the Disaster Recovery Team is appointed and trained properly, so that, even in the event that IT staff is not in the office, the team can take charge successfully.

## 2. Ownership

2.1 The Corporate Services Department is responsible for managing all computer systems for the Municipality; hence, the Corporate Services Department must make sure that in times of disasters a proper plan is in place. The Corporate Services Department is therefore the custodian of the Disaster Recovery Plan.

2.2 The designated Disaster Recovery Plan contact person is the IT Manager: The contact details of the IT Manager is as follows:

Tel (w): _____

Tel (h): _____

Cell: _____

## 3. Disaster Recovery Plan Coverage

3.1 The IT Manager, in consultation with the Municipal Manager, has authority to declare a disaster. The Disaster Recovery Team will consist of IT Manager, Chief Financial officer, Director: Corporate Services and the Municipal Manager.

3.2 The systems that the municipality have in place are:

a) The Venus Financial Management System;

b) Payday Payroll System (hosted on the Venus Server);

c) Global Information System (GIS);

d) Ultima Server (Electricity vending)

e) Domain Controller; and

f) Internet and email facilities.

3.3 All of the above systems are on different serves within the municipality.

## 4. Definitions

| | |
|---|---|
| **UPS** | Uninterruptible power supply |
| **°C** | Degrees Celsius |
| **Comfort Cooler** | An air conditioner designed to cool an environment with people in it |

| | |
|---|---|
| **Process Cooler** | An air conditioner designed to cool an environment with equipment in it |
| **ESD** | Electro static discharge |
| **False Floor** | A raised floor system, normally 600 x 600mm tiles on a electroplated under-structure |
| **Floor Plenum** | Void [space] between false floor tiles & concrete floor |
| **CVT** | Constant voltage transformer |
| **NFPA** | National Fire Protection Association |
| **LAN** | Local Area Network |
| **EMI** | Electromagnetic Interference |
| **GIS** | Global Information System |
| **Hz** | Hertz |
| **V** | Volts |
| **mS** | Milliseconds |
| **GSM** | Global System for Mobile Communications |

## 5. Emergency Contact Details of Key Persons

5.1 In the event that a problem cannot be resolved locally, the Disaster Recovery Team in consultation with the Municipal Manager and / or the IT Manager would recommend the relevant companies to be contacted to resolve the problem.

| Details | Contact Person | Telephone Number |
|---|---|---|
| Venus FMS | Business Connexion – Gideon | 0861 239 332 |
| Payday Payroll | Payday | 012 803 7730 |
| Domain Controller | First Technology (PMB) - Ben | 036 845 2300 |
| Email | AB Richards | 036 352 3792 |
| Email Forwarding System | Chimera Computing / First Technology | 036 845 2300 |
| Network and Hubs | First Technology | 036 845 2300 |
| Ultima Server (Electricity Vending) | Conlog - Waseem | 082 902 3439 |
| Internet | Telkom | 036 352 7032 |
| iShield (Internet Monitoring System) | Trade Page | 031 714 6000 |

## 6. Priority Levels of Key Systems

6.1 The municipal systems are listed below according to their priority order, the first one being:

- Venus Financial Management System
- Payday Payroll
- Domain Controller
- Network, Routers and Hubs
- Ultima Server (Electricity Vending)
- Firewall
- Mail Server & Internet Server.
- GIS Server

## 7. Deadline for Recovery

7.1 If a disaster of any kind occurs, it must only take a maximum of three days to recover data and have all users online.

## 8. Configuration Settings

| Details | Configuration Info |
|---|---|
| Venus FMS | The Venus server is a SunFire X880 server running Unix and is administered by Business Connection remotely via a 56K modem. Through this they perform maintenance and updates to the system. |
| Payroll System | The Venus server also houses the Payday payroll system which is administered by Payday. |
| Domain Controller | The Domain controller runs Windows Server 2003 Service Pack 2 and is configured in a RAID 1 configuration for data, meaning that should the primary disc fail, the data will still be intact. The operating system does not form part of the setup. Both the domain controller and the e-mail server were setup and configured by First Technology in Pietermaritzburg. |
| Email | The E-mail server also runs Windows Server 2003 Service Pack 2 and is setup to retrieve mail from our outside service provider and distribute it to all users that are setup on the system. Our service provider is Telkom with AB Richards administering the running. The municipality makes use of EFS (E-mail Forwarding System) standard edition from Chimera Computing to distribute our mail. |
| Ultima Server (Electricity Vending) | The Ultima server for electricity vending consists of two parts namely the vending coordinator and the vending server. Both machines run Windows XP Professional. The coordinator is downstairs in the machine room and is linked to the main vending server upstairs via fibre optic cable. Both machines are setup and configured by Conlog. |
| GIS Server | The GIS server is running Windows XP Professional and is administered and updated by the GIS Provincial unit. |

## 9. Preventative Measures - Server Room Setup (Safety and Security)

9.1 The table below indicates the set up of the server room, in terms of safety and security, and includes matters to be considered in future:

| Aspect | Considerations | Status Comment |
|---|---|---|
| **General Structure -** Although cost and quite a few other factors play a role when considering the actual position of the server room, one should always attempt to adhere to items such as the aspects mentioned below. | | |
| **Natural Disasters** | Server room not to be in flood stricken or structural damaged areas. | N/A |
| **EMI** | Avoid server rooms in buildings or areas that are associated with high levels of EMI or radio frequency activities such as telecommunication base stations, electrical railways, airports, etc. as certain hardware might be affected by this. EMI shielding to be installed if this is unavoidable. | N/A |
| **Pollution** | Factories and most industrial areas with high levels of dust, smoke, etc. will result in high maintenance on the filtering of the server room. | N/A |

| Aspect | Considerations | Status Comment |
|---|---|---|
| **Vibration** | Hardware might be negatively affected by continuous vibrating actions. | N/A |
| **Security** | It is always more cost affective to enhance existing security measures than to create a new system.<br>(See relevant sections below) | Not installed / Implemented |
| **Target and Risk** | Avoid windows in perimeter walls as it can have the wrong affect and could attract vandalism and / or crime to the server room. | N/A |
| **Reticulation** | In the end it must be practical to route connectivity to and from this room without having to alter surrounding areas every time a new connection point is required. | N/A |
| **Access –** Physical Access and Access Control should be considered. | | |
| **Physical Access** | Appropriate door sizes, negotiable corners from inter-leading passages, ramps and smooth floor surfaces. Proper access provided in support areas to allow for service or replacement of UPS, coolers and other large items. | Not installed / Implemented |
| **Access control:** ***Digital Key-pad System*** | Cost effectiveness and ease of installation contribute towards the popularity of this system although most systems in this range are limited when it comes to additional features. | Not installed / Implemented |
| **Access control:** ***Time & Attendance System*** | With a complete system reports can be generated on the actual access gained during a determined period, as cards are assigned to authorised staff. This can also be integrated in order to operate via the same cards or tags if a main access / security system already exists. | Not installed / Implemented |
| **Flooring -** Flooring is crucial in the sense of anti-static qualities, load bearing capabilities as well as practicality when considering cabling reticulation and air conditioning within the server room. One can consider any one of the following two options mentioned below. | | |
| **Raised Floor** | A raised floor system is preferred and the void is used for air conditioning as well as cable reticulation whilst laminated floor tiles will provide a sturdy, ant-static base to house the equipment & cabinets. The concrete or building floor needs to be sealed with an approved sealer in order to maintain a dust free environment. The depth of the floor void [plenum] should ideally be 600mm and not less than 400mm if ventilation and cooling are to be applied via the void and perforated floor tiles. Neatness of cable reticulation is of utmost importance to ensure that airflow passages are not blocked, as it will result in hot spots being generated above the floor. Custom cut-outs in order to accommodate cable entries must be fitted with the necessary protection on the edges and "self sealing" openings are required to maintain the pressure within the void. It must be ensure that the floor structure is able to withstand the equipment and cabinet weight planned for the server room. | Not installed / Implemented |
| **No Raised Floor** | Sometimes limiting factors such as lower than normal ceiling heights, which make the installation of a raised floor system impossible. In the event that no raised floor is installed, the floor covering should be of an industrial, vinyl-type finish with similar anti-static qualities. The tiles are normally 2mm in thickness and measuring 608 x 608mm. When the correct conductive adhesive is applied, a conductive flooring system can be achieved whereby potential harmful static charges are dissipated through the tile via conductive pathways and eventually through the adhesive to an electrical earth point without the inclusion of a copper grid underneath the tiles. | Not installed / Implemented |
| **Temperature and Humidity -** As seen in the flooring section, centres that do not have raised floor systems installed may be encountered and where cabinet density is very low due to less hardware requirements. In this case under floor ventilation and cooling would not be possible or cost effective. It is then required to ensure that the same levels of cooling are obtained / maintained with process type air conditioners installed in the correct manner. | | |
| **Coolers** | Equipment gets cooled via process coolers whereas humans or workspace areas rely on comfort coolers – in simple terms the difference being the human body putting heat & water [sweat] into the air whereas equipment only dissipate heat. | Currently there is an inadequate "comfort cooler" type air-conditioner installed in the server room. |

<table>
<tr><th>Aspect</th><th>Considerations</th><th>Status Comment</th></tr>
<tr><td>Process Air Conditioners vs. Comfort Air Conditioners</td><td>Process air conditioners are designed to operate 24 x 7 compared to comfort coolers that have been designed for an 8 x 5 time frame. Incorrect application could result in comfort coolers operating for too long periods, which in turn will result in major repair work required after a relatively short period of time. The air filtration via a process cooler is of a much higher standard due to specific filter and fan applications that could not be achieved with comfort coolers. Air conditioning must be rated according to the heat load generated within the room with at least 35% spare capacity available.</td><td>Not installed / Implemented</td></tr>
<tr><td>Humidity</td><td>Humidity should be controlled and kept between 45 to 50%. If the humidity drops below 45% electro static discharge [ESD] may be encountered, whilst a level of more than 50% would result in corrosive problems associated with high humidity levels.</td><td>Not installed / Implemented</td></tr>
<tr><td>Temperature</td><td>The acceptable temperature levels are between 21°C and 23°C. Data centres and server rooms require process cooling for a number of reasons:<br>- The heat load in a computer room is very dense. Data centres generally have up to 8 x the heat density of offices or a workspace environment.<br>- The heat load in a data centre varies from area to area, depending on the layout within the room. The cooling system must be able to address the specific needs of each piece of equipment.<br>- The data centre heat load will change when additional hardware is added and the cooling system must be adaptable to such changes.<br>- The data centre cooling system must provide for adequate change of air in the conditioned space. While a normal office-cooling environment requires only 2 x air changes / hour, the high-density heat load in a data centre could require as many as 30 x changes / hour.</td><td>Not installed / Implemented</td></tr>
<tr><td colspan="3">Electrical Requirements - Careful & detailed planning is required in order to provide a means of adequate, reliable & stable power source to the equipment. These parameters are usually strictly followed in the early stages but overlooked when hardware alterations are implemented. A direct result of this is that electrical circuits are left out of the picture when additional hardware is installed and socket extension units or so-called “double-adaptors” are used when the need to connect arises. This is a huge risk as one faulty circuit could leave a multitude of equipment in the dark. Apart from this, overloading of the circuits in this manner is creating a fire & safety hazard.</td></tr>
<tr><td>Normal Supply</td><td>This is the connection received on site from the supply authority. Although the municipality does not have much control over the quality of the connection, the electrical supply should be within defined parameters and the critical rating of each centre will determine whether the room can operate on the normal electrical supply or whether a standby generator and / or UPS would be required. Only in cases with absolutely noncritical hardware, one would consider operating only via the normal feed. It does, however, occur that, through accidents, copper theft or even planned shutdowns that power failures and surges are experienced (that were not anticipated) – hence the need for standby generators or even UPS modules.</td><td>The municipality cannot operate using only the normal feed supply. There is a need for a UPS.</td></tr>
<tr><td>Constant Voltage Transformers (CVT’s)</td><td>If the municipality can accept interruptions but power fluctuations are not inside the relevant parameters (see below), the municipality can consider the application of constant voltage transformers [CVT’s], or other means of voltage / supply stabilisers.<br><br>Some guidelines with regards to acceptable fluctuations in South Africa:<table><tr><td>Frequency:</td><td>49,5 – 50,5 Hz</td></tr><tr><td>Supply voltage:</td><td>198 – 231 V</td></tr><tr><td>Impulses:</td><td>550 V</td></tr><tr><td>Sags:</td><td>0 V for less than10mS</td></tr></table></td><td>A study should be done to determine the nature and cause of fluctuations in order to determine whether a CVT is necessary.</td></tr>
</table>

| Aspect | Considerations | Status Comment |
|---|---|---|
| **Uninterruptible Power Supply (UPS)** | The municipality cannot afford to have the server room interrupted without having known about the interruption beforehand, as certain hardware or data might be lost due to actions of this nature. However, the municipality may be able to accept an interruption if it were able to shut down operations in a more planned and orderly fashion. | The current UPS is outdated and inadequate. A new UPS will be installed on 11 July 2009 which will service the server room and certain (red) plug-points throughout the building for a period of approximately 20 minutes in order for the municipality to switch off its systems in a safe and orderly manner. |
| **Standby Generator** | If the municipality simply cannot operate without the system or the municipality stand to suffer financial losses due to the system being switched off a standby generator may be necessary. This can even be taken one step further where parallel redundant UPS systems [more than one UPS] are applied. | A standby generator is not required at this stage as a UPS is adequate (at this stage). |
| **Earthing and Bonding** | Grounding design in a server room environment must address both the electrical service as well as the equipment. The earth should not be used as the sole equipment-grounding conductor. A properly designed grounding system should have as low impedance as is practically achievable for proper operation of electronic devices as well as for safety. It is also important that the ground should be continuous from the central grounding point at the origin of the building system. Electronic equipment can be sensitive to stray currents and electronic noise. It is important to utilise a continuous, dedicated ground for the entire power system so as to avoid a ground differential between various grounds being used. All metallic objects on the premises that enclose electrical conductors or that are likely to be energised by electrical currents (e.g., circuit faults, electrostatic discharge, and lightning) should be effectively grounded for reasons of personnel safety, fire hazard reduction, protection of the equipment itself, and performance. Solidly grounding these metallic objects will facilitate over current device operation and permit return currents from EMI filters and surge suppressors to flow in the proper fashion. The common point of grounding can be connected to any number of sources (water piping, driven earth rod, buried grid, building steel, etc.). It is important that whatever the source, the ground is carried through the entire system from this source. Ideally, the central point of grounding will be connected to multiple ground sources, such as the building steel, buried grid and cold water piping. If they are connected at the same point, there is no potential for ground loops, yet a redundancy is achieved. A water pipe used for a ground could rupture, building steel could have accumulated resistance over several floors. By tying into all of these, the possibility of a disruption is greatly minimised. | Not installed / Implemented |
| **Wiring and Cabling** | All wiring and cabling should be run in an orderly and efficient manner. This is particularly important beneath the raised floor. The nature of the server room requires frequent modifications, and it is important that obsolete cabling be removed so as to avoid airflow obstructions and to allow for future installations. Orderly cabling will minimise the potential for disruption due to disconnection of cables when work is taking place. | Not installed / Implemented |
| **Fire Detection -** A fire within the server room can have catastrophic effects on the operations of the room. The destructive force of a fire can damage equipment and the building structure beyond repair. The contamination from a smouldering fire can also have damaging effects on the hardware, and can carry heavy costs in repairs. Even if the actual fire is avoided, discharge of the fire suppression medium can have a damaging impact on hardware. Whether measured in their threat to human safety, damage to computer equipment or loss of business due to systems disruption, the costs of a fire can be staggering. Numerous steps can be taken to avoid the risk of fire in the server room environment. Compliance with NFPA 75 will greatly increase the fire safety in the server room. The precautions mentioned below should be taken into consideration in the design and maintenance of the server room and support areas. | | |
| **Unnecessary Storage** | Avoid unnecessary storage. Combustible materials should be avoided in the server room. Only the minimum supplies absolutely necessary to the functioning of the room should be kept within its perimeter. Packing materials and other unnecessary items should be removed as soon as possible. | Not installed / Implemented |
| **Air-Conditioners** | Reheat-coils on the air conditioners should be checked periodically. If left unused for long periods of time, these can collect layers of dust that smoulder or ignite when the unit is called for. | Not installed / Implemented |

| Aspect | Considerations | Status Comment |
|---|---|---|
| **Penetrations** | The room perimeter should be inspected periodically for penetrations. Penetrations can expose the serer room to influences from more loosely controlled areas. An alarm or suppression system discharge caused by conditions outside the Server room is unacceptable. | Not installed / Implemented |
| **Smoke Detectors** | Computer room fires are often small or smouldering, with little effect on the temperatures in the room. The smoke itself can impact the computer hardware, and it is necessary to employ a detection system that is sensitive to smoke and other products of combustion rather than temperature. The specific detection and extinguishing system is dependent on the specific design and exposures of the individual server room area. NFPA 75 regulations should be applied as far as possible. | Not installed / Implemented |
| **Suppression Systems** | A passive suppression system reacts to detected hazards with no manual intervention. The most common forms of passive suppression are sprinkler systems or chemical suppression systems. Sprinkler systems can be flooded (wet pipe) or pre-action (dry pipe). A flooded system incorporates pipes that are full at all times, allowing the system to discharge immediately upon threat detection. A pre-action system will flood the sprinkler pipes upon an initial detection, but will have a delay before actual discharge. Chemical total flooding systems work by suffocating the fire within the controlled zone. | Not installed / Implemented |
| **Chemical Flooding Repression Systems** | Chemical total flooding systems work by suffocating the fire within the controlled zone. The suppression chemical most often found in server rooms has always been Halon 1301. Halon has now been eliminated in favour of the more environmentally friendly FM200, NAF SIII. Carbon dioxide [$CO^2$] suppression systems are also used, but can be a concern due to operator safety issues in the instance of a discharge. These can be used independently, or in combination depending on the exposures in the room and insurance requirements. The ideal system would incorporate both a gas system and a pre-action water sprinkler system in the ambient space. The gas suppression systems are friendlier to the hardware in the event of a discharge. Water sprinklers often cause catastrophic and irreparable damage to the hardware, whereas the hardware in a room subjected to a gas discharge can often be brought back online soon after the room is purged. | Not installed / Implemented |
| **Manual Means of Suppression** | Manual means of fire suppression system discharge should also be installed. These should take the form of manual pull stations at strategic points in the room. In areas where gas suppression systems are used, there is normally also a means of manual abort for the suppression system. In designs where it is necessary to hold the abort button to maintain the delay in discharge, it is essential that a means of communication is available within reach. | Not installed / Implemented |
| **Fire Extinguishers** | Portable fire extinguishers should also be placed strategically throughout the room. These should be unobstructed, and should be clearly marked. Labels should be visible above the tall computer equipment from across the room. Appropriate tile lifters should be located at each extinguisher station to allow access to the sub floor void for inspection, or to address a fire. | Not installed / Implemented |
| **Lightning / Surge Protection -** A good quality on-line UPS with filtering on the primary side of the system will normally stop most spikes originating upstream from the UPS. This is however where the protection in this regard from a UPS ends, as it is primarily an uninterruptible power source – not, contrary to what many might believe, a device to safeguard us against the impact of lighting. | | |
| **Lightning Surges** | Lightning surges cannot be stopped, but they can be diverted. The plans for the server room should be thoroughly reviewed to identify any paths for surge entry into the room. Surge arrestors can be designed into the system to help mitigate the potential for lightning damage within the server room. These should divert the power of the surge by providing a path to ground for the surge energy. It is often easier to protect the immediate circuits entering the server. | Not installed / Implemented |

| Aspect | Considerations | Status Comment |
|---|---|---|
| **Surges Through Communications Lines** | It is also necessary to protect against surges through the communications lines. The specific design of the lightning protection system for the server room will be dependent on the design of the building and utilities and existing protection Measures.<br><br>See **Appendix A** for a graphic reflection of what should / could be done. | Not installed / Implemented |
| **Remote Monitoring / Environmental Control -** Accurate and comprehensive monitoring of environmental support equipment and in-room conditions is extremely important in an environment as complex and sensitive as a server room. The monitoring system used must effectively assess the room conditions, or it will provide an inaccurate representation that can lead to inappropriate actions or ill-founded assumptions. | | |
| **Room Condition Sensors** | The system in place must provide a detailed and representative profile of room conditions. If a single point of reference is used, it will not give an accurate picture of the room's profile. If a single sensor is placed in an area with appropriate conditions, such as on a column directly above a perforated tile, the monitoring system would be indicating that room conditions are appropriate even though this may not be the case. Assumptions concerning the environment that are based on such data can lead to decisions that could actually degrade conditions. The same can be said about a multi-point system that has inappropriately placed sensors. | Not installed / Implemented |
| **Historical Trends** | The system should have historical trend capabilities. The data gleaned from analysis of historical psychometric information can be instrumental in determining seasonal changes or other outside influences. The data should be easily available, and the operating system should be powerful and adaptable. | Not installed / Implemented |
| **Critical Alarm Capabilities** | The system should have critical alarm capabilities. At the very least, the system should be set to notify appropriate personnel when conditions move outside certain parameters. Depending on the design of the server room, it may also be useful to have a system that performs certain functions automatically, such as switching to a back-up air-conditioner if the primary air-conditioner fails. | Not installed / Implemented |
| **Comprehensive Monitoring System** | Comprehensive monitoring systems provide an invaluable tool to building maintenance personnel. They are essential in correcting current problems in an expedient manner and identifying potential susceptibilities before they impact hardware operations. It is crucial that such a system operates totally independent from applications such as LAN connectivity, power supply, etc. in order to reflect the true readings at any given time frame. For example, although it might be preferred to see the alarm situation being displayed as a notification message via the local data network on The relevant official(s) screens, the municipality would then have to rely on the LAN to be 100% operational in order to be effective. Whilst on the other hand, if the monitoring system could operate via an external GSM or satellite means of broadcasting, the municipality would have external means of notification / communication should the municipality's infrastructure or channels be affected. | Not installed / Implemented |

## 10. Back-up Procedures

10.1 The prevention of unlawful attacks on the Council's systems is of paramount importance as is the back-up of essential data of these systems to restore the databases to their previous day's state if there should be a failure of either the hardware or the software.

10.2 Daily Back-Ups:

10.2.1 A daily back-up of both the Domain Controller and the Venus Server are to be done. The Domain Controller is to be backed-up on both magnetic tape and the hard drive.

10.2.2 The Venus server is to be backed-up on magnetic tape.

10.2.3 These back-up tapes are to be clearly labelled with the day of the week and the tapes are to be inserted at the end of the working day.

10.2.4 The back-up software will run the back-ups automatically after hours in order not to interfere with the day-to-day workings of the municipality.

10.2.5 The daily back-up tapes are stored in the server.

10.3 Monthly Back-Ups:

10.3.1 On the last working day of every month, a back-up of the Venus system will be run.

10.3.2 The magnetic tape with the back-up will be stored in a safety deposit box held at First National Bank for offsite safekeeping.

10.3.3 This is in addition to the daily back-up.

## 11. Recovery Procedures

11.1 In the event of hardware failure / loss, the relevant hardware must be replaced first, after which the relevant software must be reinstalled and reconfigured. This will be done by the relevant service providers (i.e. Venus – Business Connexion) in terms of the Service Level Agreement between the municipality and the service provider.

11.2 The most recent back-up tape is to be obtained (either from on site storage or the offsite safety deposit box).

11.3 The relevant service provider (i.e. Venus – Business Connexion) will then restore the data from the back-up tape.

11.4 Before system usage can resume as usual, test and checks have to be performed in order to ensure that the back-up was successfully restored.

## 12. Separate Recovery Site

12.1 The Municipality will, in future, look at one of the following options:

i. Buying back-up servers in the order of importance as mentioned above. All of the servers should be installed and configured to be the same as the existing machines. Once that exercise is complete those machines will be placed off-site, so that in the event that the whole building gets damaged the backup machines will just be taken from off-site, plug in and be online immediately thus minimising down time. The off-site equipment should be tested once a month to make sure that everything is in order.

ii. Installing a duplicate server off-site with a direct fibre link in order to duplicate all information in real-time. In the event of a disaster occurring and affecting the primary server(s), the duplicate server can be switched to become the primary server in a relatively short period and with minimal reconfiguration (depending on the level of destruction to the network).

# Appendix A

## Graphical reflection of Lightning / Surge Protection