

# IT Policy for Fulfilment Services

## Rationale

This document outlines the procedures in place to protect the data and systems at MMC from system failure or external interference.

Our IT planning can be sub-divided into the following categories.

- Monitoring
- Security
- Data Backup
- Redundancy

## Monitoring

The MMC IT support team operates Monday to Friday 9am to 5.30pm. During these hours they are available to assist customers via the telephone with every aspect of their fulfilment service.

MMC uses two tools to monitor its networks and services 24/7. These tools help provide a real time picture of our business.

- All of our core network hardware is monitored via ICMP every 60 seconds to ensure availability. This function is performed by a centralised web application and provides email alerting for any issues that arise.
- A more detailed analysis of server performance and readiness is completed by vendor specific application. This tool utilises SNMP to provide a low level analysis of any server performance (bottle neck) issues. This then allows us to make accurate adjustments to correct those issues. Other high dependency service such as routers and firewalls are monitored by SNMP.

Any customers who have hosted web sites with MMC will have their services monitored and verified by the above systems.

## Security

MMC takes a multi tiered approach to its virus and security protection in order to prevent failure or loss due to malicious attack.

- Anti virus protection software has been installed on all workstations and servers to monitor data flows from electronic sources.
- Access protection software has been installed on all workstation and server to block unwanted or malicious activity. This software also prevents unwanted programmes from operating.
- Both of the above services are centrally controlled and updated to include the latest vulnerabilities on a daily basis.
- Windows security updates are automatically distributed to vulnerable PC's and servers. Updates are pushed every day to ensure that any security issues are quickly resolved.

- MMC utilises an email smart host service for all its inbound and outbound email. This service monitors email traffic and quarantines any infected email or email suspect of being spam.
- MMC uses a hardware firewall at the edge of its networks to provide stateful packet inspection for all external data transfers. This service protects the internal networks, including the DMZ / PSN where web and FTP services are based. MMC employed a strict firewall policy to ensure that no internal service (protected or PSN) are over exposed to public access.

## **Data Backup**

### **Internal Data**

Internal data is server data that resides on the protected network (everything on the private side of the firewall). This data is backed up using two methods.

- MMC replicates all of its internal data to a mirror server every 15 minutes. The mirror server then takes a snapshot of this data 4 times a day on a 30 day cycle. This means we have a maximum data loss window of 15 minutes. It also means we can recover to any point in the last 30 days to within 6 hours.
- The second system used for data backups is a tape system. Every evening the tape backs up all of the internal data on a 30 day cycle. These tapes are held onsite in a fire safe.

### **External Data**

External Data is the data that resides in the DMZ / PSN (public) areas of our network. This includes FTP, website and SQL data. This data is dealt with in a variety of ways

- **FTP Data**  
Not backed up. This data only passes briefly through this service, either inbound to our protected network or outbound to somebody else's.
- **Website Data**  
Backed up on a daily basis to a local device, 7 day cycle. There is always a copy of this data on the protected network which is maintained under the internal data policy
- **SQL Data**  
Backed up on a daily basis to a local device, 14 day cycle. There is always a copy of this data on the protected network which is maintained under the internal data policy

## **Redundancy**

### **Redundancy Procedure**

MMC plans for a level of redundancy in all of its core hardware infrastructure.

- ISDN telephone lines

MMC operates two ISDN 30 lines which dynamically load balance incoming and outgoing calls.

- Internet \ data connections  
MMC uses a 2mb leased line as its primary source of connectivity. A 2mb ADSL line is used as a backup in case of failure.
- Domain services  
Two domain controllers with mirrored services provide continuity of service in case of failure.
- Data servers  
As discussed in detail in "Data Backups".
- Power Supply  
Emergency power is handled in two parts. Every networked piece of hardware (PC, server, router etc) is supported by a UPS. High availability services such as servers are supported by managed UPS to allow for real-time monitoring and reporting. In addition to this MMC has two onsite generators to provide long term emergency power.

#### **Publishing and reviewing this document**

This document is to be reviewed on a sixth monthly basis. Updated copies are circulated to all IT staff and directors. This document was last reviewed on 15<sup>h</sup> April 2009.

#### **Audit of security procedures**

An audit of security and backup procedures should take place every six months to assist with the review of this and other policies. This audit should include information on the previous six months logged activity, monitoring reports and recommendations for upgrades and improvements to the security procedures.