|  |
| --- |
| Backup Policy vs Backup Plan vs Backup Procedure |
| Backup Policy  Schedule |
| |  |  |  | | --- | --- | --- | |  |  | User manual | |

1. Purpose of this document is to ensure that a consistent procedure is used for the backup of critical for the company data:
   1. Backups are in place to ease system recovery in case of a major disaster or hardware failure.
   2. Backups are in place to help recovery of vital systems and applications for the company as well as important documents.
2. Scope
   1. This document is applicable to MakeItWork4You and covers OS, applications, logs, critical devices and files.
3. Backup Policy
   1. Backup should be made on a regular basis that will ensure the continuity of processing in the event of a processing interruption.
   2. All backups must be recorded, identified and securely stored and disposed following secure procedures.
   3. Copies of backup files and documents must be kept off-site in a secure location.
   4. There should be a periodic testing of backup media at both on-site and off-site locations (at least once a year) to ensure that backup are in useable condition for recovery and that their contents are as documented. Copies of backups moved to and from off-site storage must be provided with a level of security.
   5. All backups and backup related processes must be monitored and logged.
   6. When a computer equipment is changed, consideration should be given to the backup media and data formats to ensure that they can still be restored.
   7. Automated backups must be used where applicable.
   8. The backup strategy for each system must be formally documented and approved by the system and data owners.
   9. All on-site and off-site tape must be properly labelled.
4. Restoration
   1. In the event of system failure, escalation procedure must be in place and made aware to system administrator.
   2. Recovery and restart procedures must be established and brief to relevant parties. The document must be easily accessible to the authorized parties.
   3. Source documents, reports and backup media for reconstruction of a system must be identified and documented.
   4. Restoration of the current configuration must be within agreed recovery timescales.