
# Data Backup Policy

Red Opal Innovations

Version 1

## Table of Contents

Introduction ..... 3
Data on workstations ..... 3
Responsibility ..... 3
Exceptions ..... 3
Transfer of data ..... 3
Storage ..... 3
Data on servers ..... 3
Responsibility ..... 3
Schedule ..... 3
Storage ..... 4
Naming backups ..... 4
Passwords ..... 4
Projects, rollouts, etc. ..... 4
Testing of backups ..... 4

# Introduction

This policy outlines the safekeeping of files and user data, and includes tasks such as backup and restore.

# Data on workstations

This section covers the data stored on a user's workstation and includes files stored on local storage devices, including USB drives and e-mail archives.

## Responsibility

Each individual user is responsible for data stored on their own desktop computer/workstation. This means that users should regularly backup data to a second location such as a removable USB hard drive, DVD or file server. The IT Department is unable to complete the backup on the behalf of a user, as the data is the responsibility of the user. The IT Department is able to provide training in how to complete a backup, if required.

## Exceptions

If the IT Department is required to complete any major work on a workstation which could affect the data stored on the local drives, the IT Department will backup any files prior to starting any work. This will involve creating a second backup of the computer's hard drives using Macrium Reflect.

## Transfer of data

When user data needs to be transferred from one PC to another, the IT Department will use the Windows Easy Transfer (WET) tool to assist in the backup/restore of files and data.

## Storage

Users will be required to store backups on external USB hard drives or flash drives. When using the WET tool, the IT Department will store the archive file on either a hard drive or flash drive, as this is a temporary measure during the transfer of data.

# Data on servers

This section covers the data stored on a server, including departmental, personal (home) and public shared folders. It also covers user accounts and e-mail, including attachments, stored on ROI servers.

## Responsibility

Data stored on ROI servers is the responsibility of the IT Department and it is recommended that all important company data be stored in appropriate shared folders/network drives.

## Schedule

Files on ROI servers are backed up on a nightly basis. Files are backed up incrementally and scheduled for 9pm each night. This ensures that the backup does not impact upon server speed or availability during working hours.

### Storage

All backups are stored away from the servers in a secure location. This can cause minor delays in retrieving data if a restore needs to happen.

## Naming backups

Although the file extension may change depending on the type of backup software used, all backups are to be saved using the following naming convention:

computername_date_time_type

The following example is the backup of server 1 (svr), completed on 1st February 2015 (010215) at 10pm (2200). The backup type was incremental (inc):

srv1_010215_2200_inc

The following example is a full backup of desktop PC ROI-SAM-06. It was completed at 9am on the 1st February 2015:

ROI-sam-06_010215_0900_full

The following is an example of a Windows Easy Transfer backup of the PC ROI-SAM-06 completed at 1:30pm on 1st March 2015:

ROI-sam-06_01032015_1330_wet

## Passwords

Where applicable, passwords will be set on archive files to ensure security.

## Projects, rollouts, etc.

If the IT Department is working on special projects, any plans and policies covering those projects will outline additional information regarding backups.

## Testing of backups

Where the IT Department is responsible for backups, testing will be done on a regular basis to ensure the integrity of the backups. Server backups will be tested by restoring the data to a test server, then verifying the restored files.

Where the IT Department backs up a workstation as a part of major works or projects, the backup will be tested by restoring it to a spare hard drive and testing the restored files.