



Plastica Ltd

Data Backup Policy

Date: 18/01/24

Version: 4

HS&E 22

Notes:

Added ransomware protection to user shares and SQL backup was extended to differential for every day of the week

Contents

	Page Number
1.0 Purpose and Objective	3
2.0 Scope	3
3.0 Key Data	3
4.0 Backup Frequency and Retention	3
5.0 Backup Testing	4
6.0 Backup Storage and Cloud Environment	4
7.0 Legal and Regulatory Obligations	4
8.0 Reporting	4

1.0 Purpose and Objective

Plastica have developed this backup plan to be used in the event of a significant disruption and in accordance with the DRP and in the recovery of user files that may have been deleted. The goal of this plan is to outline the key steps to be performed to ensure should it be required Plastica can restore loss data

2.0 Scope

The scope of this plan is to outline what data is backed up, when it is backed up and how the integrity of those backups are tested.

3.0 Key Data

Plastica have identified the following data as key data and should be included in backups to enable the recovery of the data should it be required

AX SQL Database – located on PLAS-SQL, databases AX2012Live, AX2012Live_model and RF Smart

RF Smart Server – a complete backup of the RF Smart server

Domain Controller – a complete backup of the domain controller

User files and Network Shares – backup of network user files and department shares

4.0 Backup Frequency and Retention

Plastica have identified the following backup frequency and retention of each set of data in order that in the event of loss of data, the amount of data lost is kept to a minimum

AX SQL Database – Full backup every weekday evening, during the period of 6am to 8pm every day a Differential backup and transaction backup will take place every 5 minutes.

Data held for 30 days or 28 full backups whichever is the greatest

RF Smart SQL Database – Full backup every weekday evening, during the period of 6am to 8pm every day a Differential backup and transaction backup will take place every 5 minutes.

Data held for 30 days or 28 full backups whichever is the greatest

RF Smart Server – Bare metal backup once a week, 2 full backups are retained

Domain Controller – Bare metal backup every evening, 7 days a week, 3 full backups are retained

User files and Network Shares – backup takes place every evening, 5 versions of each file are retained and for 365 days after the user deletes a file locally

5.0 Backup Testing

Plastica have identified the following testing procedure to ensure the integrity of backups

AX SQL Database – Tested periodically on onsite test server

RF Smart SQL Database – Tested periodically on onsite test server

RF Smart Server – Tested and verified periodically

Domain Controller – Tested and verified periodically

User files and Network Shares – Periodic testing of random files restored to NAS drives

6.0 Backup Storage and Cloud Environment

Plastica utilise the Amazon AWS storage system for all backups, once backups have been completed they are immediately transferred to Amazon.

All backups are compressed and encrypted

For cloud testing and backup server Plastica utilises Amazon EC2

7.0 Legal and Regulatory Obligations

Plastica shall comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (2018)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000 Freedom of Information Act 2000
- PCI Compliance

8.0 Reporting

The IT department shall report to the Directors if there is an issue with the backups which may impact on the company's ability to recover data. They will also report to the directors about any issues regarding data protection.