Document ID	POL009
Document Title	Backup Policy
Author	Kevin Beadon
Version	2024.07.1
Classification	Controlled

Revision History		
Date	**Version**	**Change**
08/06/2020	1.50	Annual review
30/06/2021	1.60	Annual review
30/06/2022	1.70	Annual review
28/06/2023	1.80	Annual review
2024.07.1	2024.07.1	Annual review and new version

Distribution		
Date	**Version**	**Distribution**
08/06/2020	1.50	All staff via Intranet and Library
30/06/2021	1.60	All staff via Intranet and Library
30/06/2022	1.70	All staff via Intranet and Library
28/06/2023	1.80	All staff via intranet and Library
01/08/2024	2024.07.1	All staff via intranet, BSS website

Signed			
Date	**Version**	**Name**	**Role**
08/06/2020	1.50	Keith Richardson	CFO
30/06/2021	1.60	Dave Rawle	CTO
30/06/2022	1.70	Dave Rawle	CTO
28/06/2023	1.80	Sam Kynaston	Digital Transformation Director
30/07/2024	2024.07.1	Jack Watson	Managing Director

Contents

Introduction

The purpose of this Policy is to:

- To safeguard the information assets of Bytes Software Services (Bytes/Company).
- To prevent the loss of data in the case of an accidental deletion or corruption of data, system failure, or disaster.
- To permit timely restoration of information and business processes, should such events occur.
- To manage and secure backup and restoration processes and the media employed in the process.

The retention periods of information contained within system level backups are designed for recoverability and provide a point-in-time snapshot of information as it existed during the time defined by system backup policies.

Backup retention periods are in contrast to data retention periods defined in the GDPR Data Register

System backups are not meant for the following purposes:

- Archiving data for future reference.
- Maintaining a versioned history of data.

Scope

This Policy, and supporting procedures, encompasses all system resources and supporting assets that are owned, operated, maintained, and controlled by Bytes and applies to all servers and data (on-premise or cloud) that is managed by Bytes.

Policy Details

Overview

This Policy is set out to identify how Bytes Software Services safeguards important information in case of data loss, etc and to outline frequency and how long backups are retained.

Lines of Responsibility

All users – Ensuring that data stored on Bytes-provided devices such as laptops is copied to the File Servers ready for backup. Data on user devices are not backed-up unless copied to Bytes File servers.

Systems Support Team is responsible to the Head of IT and they:

- Ensure facilities are available.
- Ensure sufficient backup space is available.
- Take overall responsibility for trust adherence to this Policy.
- Check the backup log for completion, be responsible for the safekeeping and availability of all back-up media and logs.
- Perform test/live restores.
- Report any backup failures to the Head of IT and log accordingly and investigate any reported exceptions.

Head of IT (or equivalent) is responsible for ensuring that the backup Policy is adhered to and any new systems follow this Policy. Escalation is to the Financial and Operations Director (or equivalent).

Chief Technical Officer (or equivalent) has Board level responsibility for ensuring that Bytes Software Services data is backed-up according to the business need.

Review of Policy

Head of IT (or equivalent) and the Financial and Operations Director (or equivalent) are responsible for reviewing the backup Policy annually or after a serious issue.

Systems Backup

Bytes has the following types of backup data:

- File Server – Unstructured data located on Bytes fileservers
- E-Mail – E-mail data stored on-premise on Exchange 2016
- Database – All structured data contained on database
- SharePoint – Unstructured data stored on Azure Cloud service
- Virtual Machine – All data stored on a virtual server including the Operating System and data

Backup details of the various backup data types:

- File Server
    - Frequency: Daily
    - What is backed up: Changed data
    - Retention:
        - Minimum of 30 days and Maximum of 60 days
        - After 60 days backup is rolled-up to one full 30-day backup
        - Each 30-day full backup is retained for 12 months (12 x Monthly backups)
- E-mail
    - Frequency: Daily
    - What is backed up: Changed data
    - Retention:
        - Minimum of 30 days and Maximum of 60 days
        - After 60 days backup is rolled up to one full 30-day backup
- Database
    - Frequency: Daily
    - What is backed up: Full data
    - Retention:
        - Minimum of 30 days and Maximum of 60 days
        - After 60 days backup is rolled-up to one full 30-day backup
        - Each 30-day full backup is retained for 12 months (12 x Monthly backups)
- SharePoint/Office 365
    - Frequency: Daily
    - What is backed up: Changed data
    - Retention:
        - Minimum of 30 days and Maximum of 60 days
        - Each 30-day full backup is retained for 12 months
- Virtual Machines
    - Frequency: Snapshot every 4 hours
    - What is backed up: Changed data
    - Retention:
        - 2 days

Exceptions are as follows:

- Door Entry System (SQL)
    - Frequency: Monthly
    - What is backed up: All data in the SQL database
    - Retention:
        - 2 Months

Transportation and Storage of Backup

- All production backup data is stored at Bytes Leatherhead office and off site at the DR datacentre, Croydon.
    - Exceptions are the 12 monthly backups which are stored at the DR datacentre only
- All backup data is written to disk
- A copy of the backup data is made on a non-Microsoft file system
- File, E-mail, SQL backup data is maintained by Attix Backup system
- Attix backup is encrypted in transport and at rest using AES256
- SharePoint/Office 365 is backed-up using Synology Backup from Azure and replicated to the DR site
- Virtual Machine backups are maintained using NetApp SnapMirror.
- All data is transported to the DR datacentre across encrypted VPN.
- File, E-mail, SQL and SharePoint/Office 365 data is stored on the production datacentre for a minimum. of 30 days and a maximum of 60 days. All other backup data is located off site at the DR datacentre only.
- All Virtual Machine backup data is located at the production and DR datacentre.
- Expired backup data is deleted automatically.

Disposal of Media

Bytes Software Services only store data on disk and therefore the backup media is regarded as the disks storing the backup data.

- Prior to retirement and disposal, Systems Support will ensure that:
    - The media no longer contains active backup images.
    - The media's current or former contents cannot be read or recovered by an unauthorised party.
- Backup media (the disk storage holding the backup data) is destroyed and recycled in accordance with the Waste, Electrical and Electronic Equipment Directive 2012/19/EU and records maintained.

Validation

- Daily, logged information generated from each backup job will be reviewed for the following purposes:
    - To check for, and correct, any errors.
    - To monitor the duration of the backup job.
    - To optimise backup performance where possible.
- Systems Support will identify problems and take corrective action to reduce any risks associated with failed backups.
- Random test restores from the production datacentre will be carried out once a month to verify that backups have been successful
- Random test restores from the DR datacentre will be carried out once every three months to verify that offsite backups are valid
- IT will maintain records demonstrating the review of logs and test restores so as to demonstrate compliance with this Policy for auditing purposes.

Data Recovery

- Requests for data recovery is made using any of the following methods:
    - E-mail helpme@bytes.co.uk
    - Call 01372 418504
    - Web https://helpme.bytes.co.uk
    - Visit the Systems Support team in Leatherhead
- Systems Support aim to perform data restore requests within 1 working day.