Benifex
A Zellis Company

SyOps-19B

Record Control and Retention

Official – Commercial

Version 2.5

For more information please contact:

Head of Information Security
simonbackwell@benifex.com

Printed documents or local copies will be classified as uncontrolled documents.

Document Control

Legal Disclaimer

This document and all the information contained in it is proprietary and confidential to Benifex. Benefix reserves all intellectual property rights in relation to the material included in this document. Accordingly, it must not be disclosed or otherwise revealed to outside parties without the prior written consent of Benifex.

Version	2.5	**Status**	Live	**Last Updated**	10/02/2025	**Last Reviewed**	10/02/2025
Document Owner (Name, Title)	Simon Backwell, Head of Information Security						
Updated / Reviewed by (Name, Title)	Chris Wright, Information Security Director						
Recipients (Name, Title)	All Benifex						

See end of document for **change history**

1 Overview

All records and general documents whether digital or paper created as part of the Benifex management systems are to comply with the requirements of the ISMS and BCMS and are controlled under this procedure. Documents which specify how the ISMS / BCMS will work are controlled in line with the "Document Control Procedure".

1 Purpose

This procedure identifies the controls in place to manage the records and documents required for the Benifex ISMS and BCMS. Any changes made to the Benifex Policy, Procedures and or work instructions should be recorded in the actual document and an appropriate document for evidence of change and continual improvement.

2 Record Control

2.1 General

Every record established under this procedure must be identified as being a record within the ISMS, BCMS and general documentation. The documents must identify Benifex, the classification of document, the owner of the information and the date it was generated (or covers).

2.2 Document Referencing

Where necessary, documents are to be given serial numbers in respect to the specific subject to which they relate. The following prefixes are to be used for records relating to the ISMS, BCMS documents. Departments may use own references for local procedures where necessary.

Type of document		
Change Request: CR- (number)	Non-conformance: NCR – (number)	Corrective Action: CA – (number)
Security Incident: SI – (number)	Continuity Incident: CI – (number)	
General Business documents: Naming of documents should reflect the content		
Customer data: Named according to the data flow requirements		

2.3 Responsibilities

The following roles have responsibility for document and record retention as asset owners.

- All Asset owners are responsible for ensuring that all personal data collected, retained and destroyed is in line with the requirements of SyOps-14 and 14A.
- The Chief Finance Officer is responsible for retention of business financial related records, as well as all other statutory and regulatory records
- The Chief People Officer is responsible for retention of all HR records and the employee data required for Rewards & Benefits.
- The Head of Information Security, CTO and Employee Technology Manager are responsible for ensuring that customer employee data is appropriately protected in accordance with the GDPR requirements.
- The Chief Operations Officer and Head of Data Services are responsible for storage and retention of customer data, in line with this procedure.

- The Department Directors and associated Heads of Department are responsible for ensuring that retained records are included in business continuity and disaster recovery plans.

3 Retention

3.1 Record Protection

Records, data files and general documents are subject to the levels of protection appropriate to information contained within and are to be protected, stored, maintained and disposed of in line with the data management procedure (SyOps-14 and 14A) and document control procedure (SyOps-19A).

3.2 Customer Records

Benifex have records in various forms and there is a requirement to ensure that the records are maintained in good condition, for legal reasons and contractual reasons. Therefore, Benifex have adopted the following retention and archiving routine.

It should be noted that in some cases where a customer or representative issues a legal hold notice for documentation, it cannot be destroyed and must be separated from all other documents to ensure its safe keeping while an investigation takes place. Data in this state must not be destroyed until advised otherwise by the legal entity.

Record Type	Review Period	Remarks
Financial and Contract documents	7 years following termination of contract	Where possible documents will be scanned for electronic storage, the originals will be destroyed. Archived paper documents are to be stored in an appropriate storage facility. To be destroyed in accordance with SyOps14 and 14A
Electronic business documents	Period of Contract	To be destroyed on completion of contract
Benifex Financial Solutions (BFS)	Period of contract In accordance with FCA and NAIC all claims data and broking records are to be kept for up to five years on change of provider or termination of contract.	Unless otherwise directed by the customer or GDPR regulation overrules requirements.
Electronic Customer PII data	**Inbound** HR files – two months TRS files - Current year and previous year (max 2 years total) **Outbound** Payroll and benefit provider reports 7 years	Customer HR files are no longer required once imported in to OneHub. The data includes all received HR files and all customer and provider reports. Files are to be destroyed using appropriate data file shredding software. Payroll and Benefit reports are to be deleted or returned to the customer at the end of the agreement. In most cases retention is 7 years while in contract

Record Type	Review Period	Remarks
SFTP	Inbound – 15 days Outbound – 15 days	This is for both customer and provider data files
Leavers	1 year (configurable)	Leaver data is pseudonymised upon leaving a customer for HR support purposes only. After the default time, data is anonymised. This is configurable per customer.
System Back-Ups	5 days	Three daily backups, maximum held is 15 copies. Thereafter, back up will be over written.
Database back ups	5 years for the Yearly back up or destroyed at end of contract if < 5 years	Database backup use GFS Policy when backing up data, this is a rotation scheme to allow for long term archiving.
Intercom Conversations	2 years	Used for Conversational Support
Telephone Voice recordings	7 years	Maintained because customers allow Benifex Employee Support Team to submit on their employee behalf when requested, this is to show approval of submission requirement.
Video	Max 2 years	Interviews associated with research and analytics
OneHub emails	30 days	Outbound email activity from SendGrid, to assist with debugging issues. Increased from 7 days.

3.3 OneHub Discounts and Cashback / Wellbeing

Record Type	Review Period	Remarks
General User data (name, email, IP address)	1 – 6 months	Kept for as long as user is valid. If user deletes account data deleted and stored for 1 month. If company terminates contract, then data removed after 6 months.
Recognition	6 months	Data removed 180 days after company has finished contract by default. Can be deleted quicker if requested. Users on recognition will not be deleted until end of contract. Otherwise, recognition service would not work and be full of blanks etc
Rewards	12 – 15 months	Reward data lists may be held up to 15 months. User has 3 months to claim the reward and 12 months to spend it.
Wellbeing	1 - 6 months	Kept if user is valid. If user deletes account data deleted within 30 days. If company terminates contract, then data removed after 180 days.
Forms/ competitions	3 months	All form or competition information submitted will be destroyed

Record Type	Review Period	Remarks
Sales User Lists	6 Months	Used for generating multiple communications, they are to be destroyed as soon as possible, or kept no longer than 6 months
CRM tickets / phone calls	7 years	Maintained for analytical and support queries
CRM contacts	If necessary for business needs.	Data will be retained for business purposes unless otherwise instructed by the data subject,
Backup data	3 years	These will not be edited. These are secured and encrypted with hosting providers
Cashback - Bank details	10 working days	Bank details are required to allow the cash back to be processed for the end user

3.4 Cloud 8 BEAM at work

Record type	Review Period	Retention Period or Criteria
EBC Client Employee Personal data, Storage of personal data within the core for an Employee Benefits Consultancy	Annually at scheme renewal	As per Licensee Agreement
Cloud 8 Supplier Information required to pay invoices and communicate regarding accounts	6 months	Until 6 months of no activity.
Cloud 8 Customer Information To pay invoices and communicate regarding accounts	6 months	After 2 years of no engagement
Others Internal documentation and records to perform day-to-day activities	Annually	7 years

3.5 Benifex Employee HR Data

Record Type	Review Period	Remarks
Career opportunity documents	12 months following unsuccessful application.	Any document associated with gaining employment fall into this category. i.e. CV, references, assessment papers etc. Candidate details should not be kept on record for other opportunities.
Termination of employment contract	6 months after termination / leaving the employ of Benifex	Any document relating to employment. i.e. NDA, Contract of employment, documents proving right to work, references,
Employee pre-employment records	Once reviewed and recorded as seen, documents do not need to be maintained as a record	Passport, proof of address, references, driving license, etc.

Record Type	Review Period	Remarks
Employment records	Maintain for period of employment contract, destroy 6 months after termination.	A letter of reference should be supplied to the departing employee, with the required details in accordance with HR procedures for references.
Employee disciplinary records	Maintain for the disciplinary period only	
Employee contracts, contract addendums and exit reference	Period of contract + 6 years	
Medical / Sickness	Period of employment only + 6 months	To ensure health and wellbeing of employee

3.6 Emails

Employees should manage their email folders, ensuring that they do not maintain information for unreasonable periods, if it is no longer required, it should be deleted. Currently email is archived after one year and remains the responsibility of the employee to manage their own mailboxes. Management of mailboxes will be monitored, and should mailbox size increase greatly, company policy may change to automated deletion from servers after an agreed period. This will be completed to ensure that any customer data that may be present within email is removed (data minimization) and / or any email relating to Benifex HR that is no longer required is deleted in accordance with an individual's rights.

The email retention policy will be agreed and can be set for individual / business requirements. Office 365 security compliance will provide labelling of documents and emails with appropriate caveats and retention periods, this has a twofold effect.

- It will automatically delete at the end of the period designated.
- Employees will not be able to delete if they attempt to delete in advance of the retention period.

3.7 Source Code / Repositories (GitHub)

Any code / repository that is no longer required is archived using GitHub's archiving functionality: https://docs.github.com/en/repositories/archiving-a-github-repository/archiving-repositories

3.8 Software Assets

The end-of-life (EOL) process for software assets will ensure software that has reached the end of vendor support or operational viability has been identified, the risks associated with continued use are assessed, and decommissioning or replacing software has been appropriate planned. This will include notifying stakeholders, documenting dependencies, and ensuring that alternative solutions or upgrades are in place to minimise disruption. Actions will be taken in accordance with SyOps-24 Change Management and the appropriate records will be documented.

Once software has been replaced and reached the EOL, Benifex will remove the availability of it to employees, any access which remains and, where necessary, update any documentation and / or records accordingly.

4 Destruction of data

All data is to be destroyed in accordance with SyOps-14 'Data management' and SyOps 14A Data Destruction.

Change History

Version	Date	Updated / Reviewed By	Page(s)	Section(s)	Description of Update
1.4	06/08/2019	Chris Wright	6	3.4	Added retention period for telephone voice recordings
1.5	17/04/2020	Chris Wright	5	2	Change to Ownership Responsibilities
1.6	01/07/2022	Chris Wright	7	3.5	Updated retention of records for unsuccessful candidates
1.7	06/10/2022	Simon Backwell	6	3.4	Intercom replaced Zendesk
1.8	28/12/2022	Simon Backwell	8	4.5	Re-ordered sections for clarity, added section 4.5 on GitHub archiving
1.9	17/01/2023	Chris Wright	6	3.3	Added Wrkit data types and period of retention.
2.0	31/07/2023	Simon Backwell	6-7	3.3	Amended Wrkit to OneHub Discounts and Cashback / Wellbeing
2.1	17/11/2023	Chris Wright	7	3.4	Included Cloud 8 BEAM at work requirements
2.2	23/05/2024	Chris Wright	5,6	3.2, 3.3	Updated BFS retention period and changed POWR to Wellbeing
2.3	11/11/2024	Chris Wright	All	All and 3,2	Replaced ISD with Head of Information Security, addition of video use and associated retention
2.4	14/01/2025	Simon Backwell	6	3.2	Added OneHub emails retention period.
2.5	10/02/2025	Simon Backwell	8	3.8	Added section 3.8 for end-of-life software.