Halo Benefits

POLICY

Business Continuity and Disaster Recovery Plan

How we keep our service running and recover from disruption.

UPDATED	VERSION	NEXT REVIEW
23 November 2026	2.0	November 2027

Halo Benefits Ltd · Owner: Chris Rees, Director · Classification: Internal & Public

Document control

Policy owner	Chris Rees, Director
Approved by	Board of Directors
Date approved	23rd November 2026
Next Review Date	23th November 2027
Review frequency	Annually
Applies to	All directors, employees and contractors of Halo Benefits Ltd, and the Halo Benefits platform
Related policies	Incident Response Plan, Risk Management Policy, Information Security Policy

Version history

Version	Date	Summary of changes	Author
1.0	30 Oct 2026	First issue	Alexander Dick
2.0	23 Nov 2026	Rebranded and restructured for clarity and readability	Dionne Clarke

Contents

1. Purpose of the plan 3
2. Scope 3
3. Our critical services 3
4. Recovery objectives 3
5. Backups 4
6. Disruption scenarios 4
7. Invoking the plan and updates 4
8. Testing 5
9. Roles and responsibilities 5
10. Compliance and exceptions 5
11. Review 5

1. Purpose of the plan

This plan sets out how Halo Benefits Ltd keeps its critical services running, or restores them quickly, when our people, offices, suppliers or technology are disrupted, including by a cyber attack.

2. Scope

This plan applies to **Halo Benefits Ltd** (company number 17577358) and covers the Halo Benefits platform, including the web application, the systems behind it, our database and the supporting services it relies on.

We do not currently hold ISO 22301 business continuity certification, and do not claim to.

3. Our critical services

We have assessed the impact of disruption to each part of our service and how we would recover it:

Service	How we recover
Customer data and uploaded files	Restored from encrypted backups into a fresh, separate database, checked, and then switched into service
Application and website	Redeployed, or rolled back to a previous working version
Sign-in and email	Recovered through our providers, with delayed messages delivered once service resumes
Optional AI and voice features	Temporarily switched off, or moved to an approved alternative provider
Team communication and source code	Named owners and backup communication channels

4. Recovery objectives

- **Data loss:** in a serious incident, we aim to lose no more than six hours of data, in line with our backup schedule.
- **Restoring service:** we aim to restore the live service as quickly as possible, and we test our recovery steps regularly to keep improving how fast we can do this.

- Our recovery objectives are approved by the Board, and any change to them needs Board approval.

5. Backups

- Full backups of our database are taken every six hours.
- Backups are encrypted with keys we control, stored privately in the UK, and kept separately from our main database provider and location.
- Backups are kept for 30 days, and all copies expire automatically within 37 days.
- Access to backups is tightly restricted and separated from day-to-day system access.
- If we ever restore from a backup, any deletion requests received since the backup was taken are reapplied, so erased personal data is never brought back.

6. Disruption scenarios

- **Loss of people or premises:** we are remote-first and use shared, documented procedures, so we do not depend on any single location.
- **Database loss, corruption or supplier failure:** we stop changes, restore a checked backup into a fresh database, run acceptance checks and then resume service, keeping the damaged copy for investigation.
- **Failed software release:** we roll back to the previous working version.
- **Cyber attack:** we contain the attack under our Incident Response Plan, remove any compromised access, preserve evidence and rebuild from a trusted release and a verified backup.
- **Wider disruption:** our service relies on providers in the UK and the EU, and we monitor them closely so we can act quickly if either is affected.

7. Invoking the plan and updates

This plan is invoked by the Head of Security & Operations, or a named deputy, who coordinates recovery under our Incident Response Plan. A named communications lead keeps employers updated throughout.

Where an incident involves personal data, affected employers are told without undue delay, and in any case within 24 hours of us becoming aware. Platform-wide outages are also posted on our public status page.

8. Testing

- We test restoring from backup into a separate, isolated environment every quarter, and can run additional tests at any time. Live customer service is not affected by these tests.
- Results are recorded and used to improve our recovery steps.
- This plan is also exercised through our annual incident response practice exercise.

9. Roles and responsibilities

- **Plan owner (Director):** owns this plan, makes sure it is tested and kept up to date, and reports on continuity risk to the Board.
- **Head of Security & Operations:** invokes the plan and leads technical recovery.
- **Engineering team:** carries out restores, redeployments and rollbacks.
- **Board of Directors:** approves our recovery objectives and accepts any remaining continuity risk.
- **Everyone:** knows how to reach the team if normal channels are unavailable.

10. Compliance and exceptions

Compliance is shown through restore test records, exercise reports and our assessment of critical services. Any change to our recovery objectives needs Board approval.

11. Review

This plan is reviewed annually, and sooner after any significant change to our suppliers or systems, and after every test or use of the plan. The plan owner proposes changes and the Board of Directors approves them.

> QUESTIONS ABOUT THIS POLICY?
>
> Contact Chris Rees, Director, or our security team at security@halobenefits.co.uk.