Halo Benefits

POLICY

Information Security Policy

Sets out how we protect the information employers and their employees trust us with.

UPDATED	VERSION	NEXT REVIEW
23 November 2026	2.0	November 2027

Halo Benefits Ltd · Owner: Alexander Dick, Head of Security & Operations · Classification: Internal & Public

Document control

Policy owner	Alexander Dick, Head of Security & Operations
Approved by	Board of Directors
Date approved	23rd November 2026
Next Review Date	23th November 2027
Review frequency	Annually
Applies to	All directors, employees, contractors and anyone given access to Halo Benefits Ltd systems or information
Related policies	Access Control Policy, Acceptable Use Policy, Data Protection Policy, Incident Response Plan

Version history

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

Contents

1. Purpose of the policy 3
2. Scope 3
3. Our security objectives 3
4. How we manage security 4
5. Classifying information 5
6. Protecting our systems and data 5
7. Certification and independent testing 5
8. Roles and responsibilities 6
9. Breaches and exceptions 6
10. Review 7

1. Purpose of the policy

Halo Benefits Ltd looks after sensitive information on behalf of employers and their employees, including pay, benefit and personal details. Protecting that information is central to how we work.

This is our main information security policy. It sets out our security objectives, who is responsible for what, and the core rules we follow. More detailed policies sit beneath it, covering areas such as access control, secure development and incident response.

We are a remote-first software company. We do not run our own data centre or office network; instead we use established, independently certified cloud providers. Our controls are practical and proportionate, and we only ever describe controls we actually operate.

2. Scope

This policy applies to **Halo Benefits Ltd** (company number 17577358), the provider of the Halo Benefits flexible benefits platform.

It covers all directors, employees, contractors and anyone else given access to our systems or information; all information we hold, in any form; and all systems we use to process it, including cloud services, source code, staff devices and AI tools.

3. Our security objectives

We aim to:

- **Protect confidentiality:** keep employer, employee, pay, dependant and benefit data private and secure;
- **Stay available:** keep the platform running and able to recover quickly, losing no more than six hours of data in a serious incident;
- **Control change:** make sure every change to the live platform is reviewed, tested and traceable;
- **Be honest:** describe our security position accurately and never claim a control or certification we do not hold; and
- **Seek independent assurance:** have our security tested and certified by independent experts.

Progress is reported to the Board at least quarterly, covering multi-factor authentication, access reviews, open vulnerabilities, staff training and backup restore tests.

4. How we manage security

Security is managed as a continuous cycle: we identify risks, put controls in place, check that they work (through access reviews, restore tests, automated build checks and penetration tests) and improve after any incident, test or review. Known risks are recorded in a single risk register, each with an owner and a target date. AI tools and AI-assisted processes are included.

This policy is supported by the following policies:

No.	Policy
02	Access Control Policy
03	Acceptable Use Policy
04	Secure Development and Change Management Policy
05	Vulnerability and Patch Management Policy
06	Supplier Security Policy
07	Data Protection, Retention and Deletion Policy
08	Incident Response Plan
09	Business Continuity and Disaster Recovery Plan
10	Security Awareness and Personnel Policy
11	Responsible AI Policy
12	Risk Management Policy

5. Classifying information

All information is handled according to one of four levels:

Level	What it covers
Public	Approved for publication, such as our website and published policies
Internal	Day-to-day business information not intended for outside the company
Confidential	Commercial information, source code, security documents and anything shared under NDA
Restricted	Customer personal data, children's data, payment records and production secrets

Confidential and Restricted information is kept only in approved systems, shared only with people who need it, and never placed in unapproved AI tools, personal accounts or removable media.

6. Protecting our systems and data

- **Assets:** We keep a register of staff devices, cloud services and code repositories, each with a named owner. When someone leaves, their devices are recovered or remotely wiped and their accounts are closed.
- **Encryption:** Data is encrypted in transit (TLS 1.2 or higher) and at rest. Backups are encrypted with keys we control and rotate annually. Passwords and other secrets are held in dedicated secret-management services, never in source code or logs.
- **Logging and monitoring:** Platform activity and security events are logged and monitored, with alerts sent to our team automatically. Sign-in security events are kept for 24 months, and employer administrators can export their own audit records.
- **Hosting and physical security:** Our live systems are hosted in the UK and EU by leading cloud providers, including AWS, TiDB Cloud and Cloudflare, whose data centres are independently certified. Staff devices must be encrypted, screen-locked and never left unattended, and any loss or theft is reported immediately as a security incident.

7. Certification and independent testing

In November 2026, Red Citadel, a CREST-accredited testing company, carried out independent penetration tests of our web application (including its API) and our external infrastructure. No

high or critical risks were found, and the external infrastructure test found no issues at all. Letters of attestation are available on request.

We do not yet hold Cyber Essentials, ISO 27001 or SOC 2 certification, and we do not claim to. Our plan is:

Item	Target	Status
CREST penetration tests (web application, API and external infrastructure)	November 2026	Completed
Cyber Essentials	Winter 2026	In progress
Cyber Essentials Plus	By February 2027	Planned
ISO 27001 readiness assessment	2027	Planned

8. Roles and responsibilities

- **Board of Directors:** approves our security policies, sets our appetite for risk and receives quarterly security reports.
- **Head of Security & Operations:** owns this policy and the risk register, leads incident response and runs access reviews.
- **Engineering team:** operates technical controls, fixes vulnerabilities and follows our secure development policy.
- **Line managers:** make sure their team completes training and follows our joiner, mover and leaver processes.
- **Everyone:** follows these policies, protects the information they handle and reports any suspected incident immediately to security@halobenefits.co.uk.

9. Breaches and exceptions

We check compliance through quarterly access reviews, automated checks, training records, restore tests and independent testing. Any breach of this policy may lead to disciplinary action or termination of contract.

Any exception must be requested in writing to the Head of Security & Operations, giving the reason and the risk. Approved exceptions are recorded in the risk register and last no longer than twelve months. Exceptions that leave a high residual risk need Board approval.

10. Review

This policy is reviewed annually, and sooner after any significant change to our platform, suppliers or the law, or after a significant incident. The Head of Security & Operations proposes changes and the Board of Directors approves them.

> **QUESTIONS ABOUT THIS POLICY?**
>
> Contact Alexander Dick, Head of Security & Operations, at security@halobenefits.co.uk.