Halo Benefits

POLICY

Access Control Policy

Sets out how we make sure only the right people can access our systems and your data.

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, service accounts and anyone given access to Halo Benefits Ltd systems
Related policies	Information Security Policy, Acceptable Use Policy, Security Awareness and Personnel 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 policy 3
2. Scope 3
3. Least privilege 3
4. Joiners, movers and leavers 4
5. Access reviews 4
6. Signing in and remote access 4
7. Privileged access 5
8. Service accounts and keys 5
9. Roles and responsibilities 5
10. Breaches and exceptions 5
11. Review 6

1. Purpose of the policy

This policy makes sure that only the right people can reach the information Halo Benefits Ltd holds, that they can reach only what their role needs, and that access is removed promptly when it is no longer needed.

2. Scope

This policy applies to **Halo Benefits Ltd** (company number 17577358) and covers all of our systems and accounts, including the Halo Benefits platform and its administration tools, our databases, cloud hosting, source code, email and collaboration tools, and the accounts we hold with suppliers.

It applies to all directors, employees and contractors, and to the automated accounts and keys our systems use to connect to each other.

3. Least privilege

We give people the minimum access they need to do their job, and no more:

- **Role-based access:** access is granted by role, and limited to the specific employers and functions that role requires;
- **Employer controls:** employer administrators can create and assign their own admin roles with detailed permissions, so they decide who in their organisation sees what;
- **Data separation:** each employer's data is kept separate from every other employer's, and this separation is enforced by the platform itself;
- **No automatic access:** holding a technical or support role at Halo Benefits does not in itself grant access to customer data; and
- **Individual accounts:** every person has their own named account and shared logins are not allowed. Generic or automated accounts are allowed only for system integrations and are managed as service accounts.

4. Joiners, movers and leavers

Event	What happens
Joiner	Accounts are created and access granted by role. Background screening and multi-factor authentication are completed before any access to live systems.
Mover	Access is reset to match the new role. Old access is removed rather than added to.
Leaver	All accounts are suspended on the last working day, and any keys or passwords the person could have seen are changed. Unplanned departures are handled the same day.

Requests are raised by the line manager and actioned by the Head of Security & Operations or a delegate.

5. Access reviews

Every quarter we review who holds administrative and production access, why they need it, and whether they still do. Anything no longer needed is removed. Reviews are recorded, and any issues are added to our risk register.

6. Signing in and remote access

- **Multi-factor authentication (MFA):** MFA is required for all staff accounts on our administrative and hosting systems.
- **Customer sign-in:** customer users sign in using a one-time code sent to their verified email address. Employers can also use their own single sign-on (SAML or OIDC).
- **Platform administrators:** administrators must pass a stronger sign-in check, with support for authenticator apps.
- **Passwords:** where passwords are used, they must be at least 12 characters, unique to each system, stored in a password manager and never shared or written down. Default passwords are always changed, and repeated failed sign-ins are blocked.
- **Remote access:** we have no office network. All our systems are secure cloud services, and access is decided per person and per service, not by where someone connects from. Administration tools are never left open without sign-in, and staff must use devices that meet our Acceptable Use Policy.

7. Privileged access

- Administrator rights to our core systems are held by the smallest practical number of named people, all of whom must use MFA.
- Administrator accounts are used only for administrative tasks, not everyday work.
- Changes to the live platform go through reviewed and tested code changes, not manual edits.
- Direct changes to live data are exceptional, need a stated reason and are recorded.

8. Service accounts and keys

- Automated accounts each have a named owner and hold only the permissions their integration needs.
- Passwords, keys and other secrets are stored in dedicated secret-management services. They are never written into source code, and code is automatically scanned to catch mistakes.
- Keys are changed when someone who could have seen them leaves, if exposure is suspected, and at least annually where possible.
- Secrets are never logged, or shared in chat, tickets or AI tools.

9. Roles and responsibilities

- **Head of Security & Operations:** owns this policy, manages administrator access, runs quarterly access reviews and handles leavers.
- **Line managers:** raise joiner, mover and leaver requests on time and confirm their team's access at each review.
- **Engineering team:** builds and maintains the sign-in and data-separation controls in the platform.
- **Everyone:** protects their sign-in details, uses MFA and reports any suspected compromise immediately to security@halobenefits.co.uk.

10. Breaches and exceptions

We check compliance through access review records, account records, automated checks and our sign-in system settings. Any breach of this policy may lead to disciplinary action or termination of contract.

If access cannot meet this policy (for example, a supplier that does not support MFA), it must be approved as an exception by the Head of Security & Operations, recorded in our risk register with extra safeguards, and re-reviewed at least every twelve months.

11. Review

This policy is reviewed annually, and sooner after any significant change, such as a new sign-in system or new administration tools, or after a security incident involving access. 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.