Halo Benefits

POLICY

Security Awareness and Personnel Policy

How we screen, train and support our people on security.

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, consultants and temporary staff with access to Halo Benefits Ltd systems or information
Related policies	Acceptable Use Policy, Access Control 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 policy 3
2. Scope 3
3. Screening before joining 3
4. Contracts and confidentiality 4
5. Security awareness training 4
6. Secure coding training 4
7. Training records 5
8. Changing roles and leaving 5
9. Roles and responsibilities 5
10. Compliance and exceptions 5
11. Review 6

1. Purpose of the policy

People are central to the security of a small, remote-first company. This policy sets out how Halo Benefits Ltd screens the people we bring in, binds them to confidentiality, trains them, and manages security when they change role or leave.

2. Scope

This policy applies to **Halo Benefits Ltd** (company number 17577358) and to all directors, employees, contractors, consultants and temporary staff who have access to our systems or information.

3. Screening before joining

Before anyone is given access to our systems, the following checks are completed and recorded:

Check	Who it applies to	Standard
Identity	Everyone	Government-issued photo ID checked
Right to work in the UK	Everyone engaged in the UK	A Home Office-compliant check before the start date
References	Everyone	Appropriate to the role, normally covering the last two years
Basic criminal record check (DBS or Disclosure Scotland)	Anyone with access to live systems or data	Completed before access to live systems is granted

Our platform team does not have unsupervised contact with children, so enhanced criminal record checks do not apply.

Screening is carried out in line with data protection law. Results are held securely, seen only by those who need them and kept no longer than necessary. Any disclosure is assessed against the role, not treated as an automatic bar.

4. Contracts and confidentiality

- Every employment contract and contractor agreement includes confidentiality obligations covering company and customer information, which continue after the engagement ends.
- Anyone not covered by such an agreement signs a non-disclosure agreement before receiving any confidential information.
- Contracts require compliance with our information security policies.
- New starters sign our Acceptable Use Policy before receiving access.

5. Security awareness training

Every new starter completes security awareness training within their first week, and before any access to live systems. It covers:

- our security policies and where to find them;
- handling customer data, including children's data;
- phishing and fraud, including fake payment-change and urgent requests;
- password managers, multi-factor authentication and device security;
- data protection basics and handling requests from individuals;
- approved and prohibited uses of AI tools; and
- how and when to report an incident.

Everyone repeats this training every year, updated for recent threats and policy changes. Staff are encouraged to report suspected phishing without blame, even if they have clicked a link. Any practice phishing exercises are used for learning, not discipline.

6. Secure coding training

Developers, including contractors who write code, complete secure coding training when they join and every year. It covers the industry-standard OWASP Top 10 for web applications and APIs (with particular attention to keeping each employer's data separate), handling passwords and keys safely, and the safe use of AI coding assistants, including checking AI-generated code for security flaws.

7. Training records

All training, policy sign-offs and device declarations are recorded with the date completed and the next due date. The Head of Security & Operations reviews these records every quarter and follows up anything overdue. Anyone more than 30 days overdue on annual training has their access to live systems suspended until it is complete.

8. Changing roles and leaving

- When someone changes role, their access is reset to match the new role, as set out in our Access Control Policy.
- When someone leaves, their accounts are suspended on their last working day, devices are returned or wiped, and any passwords or keys they could have seen are changed.
- Leavers are reminded of their continuing confidentiality obligations.

9. Roles and responsibilities

- **Head of Security & Operations:** owns this policy, provides training, keeps training records and confirms screening before granting access to live systems.
- **Line managers and hiring managers:** make sure screening is complete before someone starts, and that their team completes training on time.
- **Everyone:** completes training on time, follows our policies and reports concerns.
- **Board of Directors:** receives training completion figures every quarter.

10. Compliance and exceptions

Compliance is shown through screening records, signed contracts and training records. Deliberate or reckless breaches of our security policies are handled under our disciplinary procedure or the contractor's agreement. Honest mistakes that are reported promptly are treated as learning opportunities.

Someone may start before screening is complete only with the approval of the Head of Security & Operations, and only if they have no access to live systems or restricted data until it is finished. Any such exception is recorded.

11. Review

This policy is reviewed annually, and sooner after any significant change, including changes in the law on right to work or criminal record checks. 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.