Halo Benefits

POLICY

Secure Development and Change Management Policy

Sets out how we build, test and release changes securely.

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 staff and contractors who build, review or release changes to Halo Benefits Ltd systems
Related policies	Information Security Policy, Vulnerability and Patch Management Policy, Responsible AI 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. How we build software 3
4. Review and automated checks 3
5. Separate environments 4
6. Approving and releasing changes 4
7. AI coding assistants 4
8. Telling customers about changes 5
9. Roles and responsibilities 5
10. Breaches and exceptions 5
11. Review 6

1. Purpose of the policy

This policy makes sure that changes to our software and infrastructure are designed, built, reviewed, tested and released securely, and that every change to the live platform is authorised and traceable.

2. Scope

This policy applies to **Halo Benefits Ltd** (company number 17577358) and covers all source code, configuration, infrastructure and database changes for the Halo Benefits platform. It covers code written by our team and code produced with the help of AI coding assistants.

3. How we build software

Every change follows the same path:

- **Plan:** the change is described and its security and privacy impact considered. Changes affecting sign-in, permissions, personal data, payments or AI are flagged for closer review, and new uses of personal data are assessed for data protection impact.
- **Build:** work is done separately from the main codebase, never directly on it.
- **Check:** automated tests and security checks run on the change.
- **Review:** another person reviews the change before it is accepted.
- **Release:** approved changes are released through an automated process.
- **Monitor:** the platform is watched after release, and changes can be rolled back if needed.

Our secure coding follows the industry-standard OWASP Top 10 guidance for web applications and APIs. This includes checking permissions on every request, validating all input, keeping each employer's data separate, limiting request rates on public services, and keeping sensitive data out of logs.

4. Review and automated checks

- **Code review:** every change is reviewed by another person before it is accepted, with extra attention to anything affecting sign-in, data separation or security settings.
- **Automated checks:** tests, security scans and checks for accidentally included passwords or keys run automatically, and the live platform is regularly scanned for common web weaknesses.

- **Third-party components:** we use well-maintained, widely used software components, monitor them for known vulnerabilities, and fix issues under our Vulnerability and Patch Management Policy.
- **Secrets:** passwords and keys are never stored in code. They are held in dedicated secret-management services, and any secret that is accidentally exposed is treated as compromised and replaced.

5. Separate environments

- Development, testing and live systems are kept separate, each with its own credentials.
- Real customer data is never copied into development or test systems. Test data is made up or anonymised.
- Access to the live database is limited to named staff and is not used for routine development work.

6. Approving and releasing changes

Type of change	How it is approved
Standard	Approved through code review, with all automated checks passing
Significant (for example database, sign-in, permission, infrastructure or personal data changes, or new suppliers)	Also needs a written rollback plan and approval from the Head of Security & Operations, and is tested in a separate environment before going live
Emergency (fixing a live incident or actively exploited weakness)	Can be fast-tracked, but still goes through review and automated checks, and is reviewed afterwards within two working days

Every change to the live platform can be traced back to its review, its test results and its release, and releases can be rolled back if something goes wrong.

7. AI coding assistants

Our developers use AI coding assistants. The rules are:

- AI-produced code goes through exactly the same review and checks as any other code. There is no faster route.

- The developer who submits the change is responsible for it, whoever or whatever wrote it.
- AI assistants are never given access to live systems, the live database or customer personal data.
- AI assistants must never be set up to bypass reviews or checks.

8. Telling customers about changes

- Changes that significantly affect customers, such as new or changed sub-processors, changes to where data is stored, significant changes to how personal data is processed, or removal of features customers rely on, are communicated in advance, in line with the notice period in the customer agreement.
- Where an agreement sets no notice period, we give at least 30 days' notice of a new sub-processor.
- Planned maintenance likely to cause downtime is announced in advance.
- Urgent security fixes may be released without advance notice. Customers are told afterwards if the issue affected them.

9. Roles and responsibilities

- **Head of Security & Operations:** owns this policy and our review and release controls, and approves significant changes.
- **Developers:** follow this policy, write tests, review each other's changes and are responsible for the security of every change they submit, including AI-assisted ones.
- **Reviewers:** check the security impact of a change, not just whether it works.

10. Breaches and exceptions

Compliance is shown through our review history, automated check results and release records. Changes to our review and release controls are themselves treated as significant changes. Any breach of this policy may lead to disciplinary action or termination of contract.

Any exception (for example, a check that is temporarily switched off) must be approved by the Head of Security & Operations, be time-limited and be recorded in our risk register.

11. Review

This policy is reviewed annually, and sooner after any significant change to our development tools, release process, hosting or use of AI in development. 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.