Halo Benefits

POLICY

Vulnerability and Patch Management Policy

Sets out how we find, prioritise and fix security weaknesses.

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 Halo Benefits Ltd code, systems, cloud configuration and staff devices
Related policies	Secure Development and Change Management Policy, Incident Response Plan, Acceptable Use 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. Finding vulnerabilities 3
4. Assessing severity 3
5. Fixing vulnerabilities 4
6. Keeping systems up to date 4
7. Independent penetration testing 4
8. Reporting a vulnerability 5
9. Roles and responsibilities 5
10. Breaches and exceptions 5
11. Review 6

1. Purpose of the policy

This policy sets out how Halo Benefits Ltd finds, prioritises and fixes security weaknesses (vulnerabilities) in our software, the third-party components it uses, our cloud configuration and our staff devices. It also covers how we arrange independent testing and how anyone can report a concern to us.

2. Scope

This policy applies to **Halo Benefits Ltd** (company number 17577358) and covers the Halo Benefits platform in every environment, all of our source code and the components it relies on, the cloud services we configure, and staff devices.

Patching of the underlying infrastructure run by our cloud hosting providers is their responsibility, and we check how they manage it as part of our supplier due diligence.

3. Finding vulnerabilities

We look for vulnerabilities in several ways:

- automated security scanning of our source code;
- continuous monitoring of the third-party components we use for newly published vulnerabilities;
- automatic checks that stop passwords or keys from being included in code;
- regular scans of the live platform for common web weaknesses;
- cloud security monitoring, which alerts our team to suspicious activity or risky settings;
- security advisories from our suppliers; and
- independent penetration testing and reports from the public (see sections 7 and 8).

4. Assessing severity

We rate each vulnerability using the industry-standard CVSS score, then adjust it for the real risk: whether it can actually be reached, whether it is exposed to the internet, what data it could expose and whether it is being actively exploited. Weaknesses that could expose pay, dependant or health information are rated higher. The Head of Security & Operations makes the final decision on severity.

5. Fixing vulnerabilities

Severity	Our commitment
Critical and High	Treated as a priority. Open findings stop new releases until they are fixed.
Medium	Fixed within 30 days
Low	Fixed within 90 days, or formally risk-accepted in writing

If a critical vulnerability is exposed to the internet and is being actively exploited, we treat it as a security incident. Investigation starts the same day, protective measures are put in place as soon as possible (aiming for within 48 hours), and the permanent fix still goes through our normal review and checks. Affected customers are told in line with our Incident Response Plan.

Every vulnerability above Low is tracked with its severity, owner and target date. Any remediation timescales agreed in a customer contract also apply.

6. Keeping systems up to date

- The software components we use are kept on supported versions, and are upgraded before their security support ends.
- Updates go through our normal review and testing process.
- Staff devices receive operating system and browser updates within 14 days, and critical security updates as soon as practicable, in line with Cyber Essentials requirements.
- The security settings of our cloud services are reviewed against providers' recommendations at least once a year and after any significant change.

7. Independent penetration testing

In November 2026, Red Citadel, a CREST-accredited testing company, carried out independent penetration tests of our web application (including its API) and 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.

- **Frequency:** we test at least once a year, and after any major change, such as a new sign-in method, a major new customer-facing feature or a change of hosting.

- **Scope:** testing covers the customer-facing application and API, including sign-in, permissions and the separation of each employer's data.
- **Findings:** are fixed within the timescales in section 5, and critical or high findings are retested to confirm they are closed.

8. Reporting a vulnerability

Anyone can report a suspected vulnerability to **security@halobenefits.co.uk**. We will:

- acknowledge the report within three working days;
- assess it, keep the reporter updated and let them know when it is fixed; and
- not take legal action against anyone who reports in good faith, avoids accessing or changing other people's data beyond what is needed to show the issue, does not disrupt the service, and gives us reasonable time to fix it before making it public.

We do not currently run a paid bug bounty programme.

9. Roles and responsibilities

- **Head of Security & Operations:** owns this policy, sets severity, approves fixes and risk acceptances, arranges penetration tests and reports progress to the Board.
- **Engineering team:** investigates and fixes vulnerabilities within the agreed timescales and keeps software components up to date.
- **Everyone:** keeps their devices up to date and reports anything suspicious.

10. Breaches and exceptions

We measure compliance by the number of open vulnerabilities outside our timescales, reported to the Board every quarter. Any breach of this policy may lead to disciplinary action or termination of contract.

If a fix cannot be made in time (for example, because no fix exists yet), the Head of Security & Operations may approve a time-limited exception with extra safeguards, recorded in our risk register. Any critical or high exception lasting more than 30 days is reported to the Board.

11. Review

This policy is reviewed annually, and sooner after any significant change, and after each penetration test. 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.