Halo Benefits

POLICY

Risk Management Policy

How we identify, assess and manage risk.

UPDATED	VERSION	NEXT REVIEW
23 November 2026	2.0	November 2027

Halo Benefits Ltd · Owner: Chris Rees, Director · Classification: Internal & Public

Document control

Policy owner	Chris Rees, Director
Approved by	Board of Directors
Date approved	23rd November 2026
Next Review Date	23th November 2027
Review frequency	Annually
Applies to	All directors, employees and contractors of Halo Benefits Ltd
Related policies	Information Security Policy, Supplier Security Policy, Business Continuity and Disaster Recovery 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 restructured for clarity and readability	Dionne Clarke

Contents

1. Purpose of the policy 3
2. Scope 3
3. Our risk register 3
4. How we assess risk 4
5. Responding to risk 4
6. Accepting risk 5
7. When we assess risk 5
8. Keeping up with the law 5
9. Board oversight 6
10. Compliance and exceptions 6
11. Review 6

1. Purpose of the policy

This policy sets out how Halo Benefits Ltd identifies, assesses, treats, accepts and reports risks to information security, data protection, suppliers, legal compliance and our operations. It makes sure our decisions about controls are based on risk, and that the Board has a clear view of our exposure.

2. Scope

This policy applies to **Halo Benefits Ltd** (company number 17577358) and covers all risks to the confidentiality, integrity and availability of our information, our customers' information and our services, including risks from suppliers, the use of AI, changes in the law and any gaps in our own controls.

3. Our risk register

- We keep a single risk register. Each risk records its cause and consequence, the systems or services affected, an owner, the current controls, its score before and after controls, the agreed treatment and actions with target dates, and when it was last reviewed.
- Known gaps are recorded honestly, so they can be tracked and closed.
- Closed risks are kept on record with the date closed and the evidence.

4. How we assess risk

Each risk is scored on a five-by-five scale, multiplying likelihood by impact:

Score	Likelihood	Impact
1	Rare: not expected in the next 3 years	Negligible: no customer impact and trivial cost
2	Unlikely: could happen within 3 years	Minor: brief disruption, with no personal data exposed
3	Possible: could happen within a year	Moderate: limited personal data exposure or a short outage
4	Likely: expected within a year	Major: a reportable breach, a longer outage or the loss of a key customer
5	Almost certain: expected within months	Severe: a large-scale breach, exposure of children's data, regulatory action or a threat to the business

Any risk involving exposure of children's data is always scored at the highest impact.

5. Responding to risk

Rating	Score	Response
Low	1 to 4	Accept and monitor
Medium	5 to 9	Address within a planned timeframe. May be accepted by the Head of Security & Operations.
High	10 to 16	Address as a priority. Any remaining risk can only be accepted by the Board.
Critical	20 to 25	Act immediately and report to the Board without waiting for the quarterly review

For every risk above Low, the owner chooses to reduce it (by adding or improving controls), avoid it (by stopping the activity), transfer it (for example through a contract or insurance, while keeping accountability) or accept it. Actions have an owner and a target date and are tracked to completion.

6. Accepting risk

- Low and Medium risks may be accepted by the Head of Security & Operations, with the reasons recorded.
- High and Critical risks can only be accepted by the Board, recorded in Board minutes with the reasons, any conditions and a review date no more than twelve months away.
- Any exception to one of our policies is recorded as a risk and follows the same rules.

7. When we assess risk

Risks are assessed:

- at each quarterly review of the whole register;
- before any new product, feature or use of AI that processes personal data;
- before taking on a significant new supplier, and at its annual review;
- after a security incident or near miss;
- after a penetration test, certification assessment, restore test or practice exercise; and
- when legal, regulatory or threat conditions change.

Significant supplier risks, such as depending on a single provider or processing outside the UK, are carried on the same register so they are visible alongside our own risks.

8. Keeping up with the law

We monitor legal and regulatory change at least every quarter, taking external advice where needed, and record relevant changes on the register. Areas we watch include:

- UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025 and related ICO guidance, including on international transfers and AI;
- the UK Cyber Security and Resilience Bill and National Cyber Security Centre guidance;
- Cyber Essentials requirements;
- employment, right-to-work and criminal record check rules;
- HMRC and tax rules affecting flexible benefits, payroll and record keeping;
- AI regulation and guidance in the UK, and in the EU where we have EU customers or users; and
- contractual requirements from our customers, including from due diligence reviews.

9. Board oversight

- The Board receives a risk report at least every quarter, covering all High and Critical risks, changes since the last report, overdue actions, incidents, how quickly vulnerabilities are being fixed, and progress on our Assurance Roadmap.
- The Board sets our appetite for risk. We have a low appetite for risks to customer personal data and children's data, and for regulatory non-compliance.
- **Risk owners** keep their entries up to date, deliver their actions and report changes, and **everyone** raises new risks and near misses with the Head of Security & Operations.

10. Compliance and exceptions

Compliance is shown through the risk register, its review history and Board minutes recording risk reports and acceptances. There are no exceptions to the rule that High and Critical risks can only be accepted by the Board.

11. Review

This policy is reviewed annually, and sooner after any significant change to our business, products or appetite for risk. The policy owner proposes changes and the Board of Directors approves them.

> QUESTIONS ABOUT THIS POLICY?
> Contact Chris Rees, Director, or our security team at security@halobenefits.co.uk.