Halo Benefits

POLICY

Supplier Security Policy

Sets out how we choose, check and monitor the suppliers we rely on.

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 who select, manage or use suppliers on behalf of Halo Benefits Ltd
Related policies	Data Protection, Retention and Deletion Policy, Supplier Code of Conduct, Incident Response 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. Supplier risk levels 3
4. Checks before we use a supplier 3
5. Contracts and data protection 4
6. Ongoing monitoring 4
7. Ending a supplier relationship 5
8. Roles and responsibilities 5
9. Breaches and exceptions 5
10. Review 6

1. Purpose of the policy

Halo Benefits Ltd runs entirely on cloud and software suppliers, so much of our security depends on theirs. This policy sets out how we assess, contract, monitor and offboard suppliers, with particular care for sub-processors: suppliers that process personal data on behalf of our customers.

2. Scope

This policy applies to **Halo Benefits Ltd** (company number 17577358) and covers every supplier that hosts, processes, stores or can access our information or our customers' information, or that provides a service our platform depends on. Sub-processors must meet every requirement in this policy. Suppliers with no access to information and no service dependency (such as office supplies) are out of scope.

3. Supplier risk levels

Every supplier is placed in a risk tier, which decides how closely it is checked and monitored:

Tier	What it covers
Tier 1 (high)	Processes customer personal data or children's data, or our platform cannot run without it. This includes hosting, sign-in, AI, voice and communications suppliers.
Tier 2 (medium)	Holds internal confidential information or limited personal data, such as monitoring and development tools
Tier 3 (low)	No access to confidential information and no service dependency

4. Checks before we use a supplier

Before a Tier 1 or Tier 2 supplier is used with real data, the Head of Security & Operations confirms and records:

- who the supplier is and what service we are buying;
- what data it will process and why, including whether any children's data or special category data is involved;

- where the data will be processed and stored (including backups and support access), and the legal safeguard for any transfer outside the UK;
- current independent security evidence, such as an ISO 27001 certificate or SOC 2 report, which is checked rather than assumed;
- encryption, access controls and multi-factor authentication for our administrator accounts;
- how quickly the supplier will tell us about a breach, and how it manages its own sub-processors;
- how data is deleted or returned when the contract ends;
- for AI suppliers, that customer data will not be used to train their models; and
- whether a data protection impact assessment is needed.

A new sub-processor is added to our sub-processor list, and customers are given notice in line with our Secure Development and Change Management Policy, before any live personal data is sent to it.

5. Contracts and data protection

- Every sub-processor must have a data processing agreement that meets UK GDPR Article 28, covering confidentiality, security, help with data subject requests and breaches, control of further sub-processors, deletion on exit, and audit rights.
- Any transfer of personal data outside the UK must be covered by an approved legal safeguard, such as the UK International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses or UK adequacy regulations.
- The commitments we make to customers in our own data processing agreement are passed on to our sub-processors.
- Our current sub-processor list, including what each supplier does and where it processes data, is available to customers on request.

6. Ongoing monitoring

- Every Tier 1 and Tier 2 supplier is reviewed at least once a year: security evidence is refreshed and any changes to location or sub-processors are checked.
- Supplier security notices, breach reports and service incidents are monitored and handled under our Incident Response Plan.

- A significant change at a supplier, such as a breach, loss of certification or change of ownership or location, triggers an immediate review.
- Supplier risks are recorded in our risk register.

7. Ending a supplier relationship

When we stop using a supplier, we export any data we need, instruct the supplier to delete our and our customers' data and ask for confirmation, remove all accounts, keys and connections, and update our records. Customers are told when a sub-processor is removed.

Suppliers are also expected to meet our Supplier Code of Conduct.

8. Roles and responsibilities

- **Head of Security & Operations:** owns this policy and the sub-processor list, approves Tier 1 and Tier 2 suppliers and runs annual reviews.
- **Anyone choosing a supplier:** must get approval before signing up to, or sending any company or customer data to, a new service, including free tools and AI tools.
- **Board of Directors:** is told about new Tier 1 suppliers and approves any high supplier risk that is accepted.

9. Breaches and exceptions

Using an unapproved supplier with customer data is treated as a security incident. Any breach of this policy may lead to disciplinary action or termination of contract.

If a supplier cannot meet a requirement, the Head of Security & Operations may approve its use, with the gap recorded in our risk register and disclosed to customers where it affects them.

10. Review

This policy is reviewed annually, and sooner after any significant change, including any new type of sub-processor. 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.