Halo Benefits

POLICY

Incident Response Plan

Sets out how we respond to security incidents and keep customers informed.

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 and contractors of Halo Benefits Ltd
Related policies	Business Continuity and Disaster Recovery Plan, Data Protection Policy, Vulnerability and Patch Management 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 plan 3
2. Scope 3
3. Reporting an incident 3
4. Severity levels 3
5. Our response team 4
6. How we respond 4
7. Telling customers 4
8. Telling regulators and others 5
9. Evidence and testing 5
10. Compliance and exceptions 5
11. Review 6

1. Purpose of the plan

This plan sets out how Halo Benefits Ltd detects, responds to, recovers from and learns from security incidents and personal data breaches, and how and when we tell customers, the Information Commissioner's Office (ICO) and others.

2. Scope

This plan applies to **Halo Benefits Ltd** (company number 17577358) and covers any event, including a suspected event, that threatens the confidentiality, integrity or availability of our information, our customers' information or our services.

Examples include unauthorised access, a compromised account, leaked passwords or keys, malware or ransomware, data sent to the wrong person, a lost or stolen device, a supplier breach affecting our data, and outages of the Halo Benefits platform.

3. Reporting an incident

Anyone who suspects an incident must report it immediately to **security@halobenefits.co.uk** and to the Head of Security & Operations directly. They must not investigate alone, delete evidence or contact anyone affected until the Incident Lead decides how to proceed. Customers and members of the public can use the same address.

Every suspected incident is logged, whether or not it turns out to be serious.

4. Severity levels

Level	What it means	Response
Critical	Confirmed or highly likely compromise of customer personal data, or a full platform outage	Immediate, with the Board informed the same day
High	A significant risk to customer data, or a major feature unavailable for many customers	Within 2 hours, with the Board informed within 24 hours
Medium	A contained issue with limited impact	The same working day
Low	A minor issue with no customer impact	The next working day

Severity is set when the incident is first assessed and updated as more facts become known.

5. Our response team

As a small team, one person may hold more than one role, and a named deputy steps in if the Head of Security & Operations is unavailable.

- **Incident Lead** (Head of Security & Operations): decides severity, directs the response and approves all notifications and closure.
- **Technical Lead** (senior engineer): investigates, contains the problem and restores service.
- **Communications Lead:** prepares and sends updates to customers and staff once approved by the Incident Lead.
- **Record keeper:** keeps a timed record of facts, decisions and actions.
- **Board of Directors:** is informed of all critical and high incidents and makes decisions affecting the business as a whole.

6. How we respond

- **Detect:** through automated security monitoring and alerts, supplier notifications, and reports from customers and staff.
- **Assess:** confirm whether an incident has happened, set its severity, identify the systems, data and customers affected, and record when we became aware.
- **Contain:** limit the damage, for example by disabling accounts, changing exposed passwords or keys, blocking harmful traffic or taking a feature offline, while preserving evidence.
- **Fix:** remove the cause, such as fixing a weakness or removing unauthorised access.
- **Recover:** restore normal service, including from secure backups where needed, and monitor closely for any recurrence.
- **Learn:** for every critical or high incident, and any incident affecting customers, we complete a review within ten working days. It records what happened, the root cause and the actions we will take, which are tracked to completion.

7. Telling customers

- If an incident affects a customer's data or service, we tell them without undue delay, and in any case within **24 hours** of becoming aware of a personal data breach.

- Our notice gives the employer what it needs for its own assessment: what happened and when, the data and people involved, the likely consequences, what we have done and plan to do, and a contact. Anything not yet known is provided as soon as it is available.
- Where a customer contract sets a shorter timescale or specific requirements, the contract applies.
- Platform-wide outages are also posted on our public status page.
- All external statements are approved by the Incident Lead, and are factual rather than speculative.

8. Telling regulators and others

- Where we are the data controller and a breach is likely to put people at risk, we tell the ICO without undue delay and within 72 hours of becoming aware. Where there is a high risk to individuals, we tell them directly.
- Where we process data on behalf of an employer, the employer decides whether to notify the ICO and individuals, and we support them fully.
- Where appropriate, we also inform the police or Action Fraud, the National Cyber Security Centre, our insurer and affected suppliers.
- Decisions not to notify are recorded with the reasons.

9. Evidence and testing

- Logs and records relating to an incident are preserved securely for the life of the investigation and any related claim.
- This plan is tested at least once a year through a practice exercise, rotating through scenarios such as ransomware, a compromised administrator account and a supplier breach. Results are recorded and the plan is updated.

10. Compliance and exceptions

Failing to report a known incident is a disciplinary matter. During a live incident, the Incident Lead may depart from this plan where necessary, and the reasons are recorded.

11. Review

This plan is reviewed annually, and sooner after any significant change, after every critical or high incident and after each practice exercise. 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.