Incident Response Procedure

Personal data breaches and security incidents

Version 1.0 · 29 June 2026 · Kaizen Kanri (KVK 42049431)

1. Scope and commitment

This procedure applies to any incident affecting the confidentiality, integrity or availability of customer data in the Kanriva™ platform or the FlowCrew™ worker app.

Kaizen Kanri commits to notifying an affected customer of a personal data breach **without undue delay and in any event within 48 hours** of becoming aware of it. That commitment is contractual: it appears in clause 9 of the Data Processing Agreement.

Under the GDPR the customer is the controller. The customer decides whether a breach is reported to the supervisory authority (in the Netherlands, the Autoriteit Persoonsgegevens) and whether data subjects are informed. Kaizen Kanri's role is to detect, contain, inform and assist — not to decide on the customer's behalf.

2. Severity classification

Level	Definition	Examples	Customer notification
S1 — Critical	Confirmed unauthorised access to or loss of personal data, or confirmed cross-customer data exposure	Account compromise with data access; a defect returning another tenant's records	Immediately on confirmation, and in any event within 48 hours
S2 — High	Credible suspicion of unauthorised access, or loss of data integrity affecting operational records	Anomalous access pattern; corrupted schedule or presence data	Within 48 hours of becoming aware
S3 — Moderate	Security-relevant defect or misconfiguration without evidence of data exposure	Permission check too permissive, found internally and fixed	In the next release note, or immediately if the customer is affected
S4 — Availability	Platform unavailable or materially degraded, no data exposure	Hosting outage, failed deployment	As soon as the cause is known, with an expected restoration time

An incident is escalated, never quietly downgraded. If the classification changes, the customer is told that it changed and why.

3. Procedure

Step 1 — Detect and record (immediately)

The incident is recorded with the time of discovery, how it was discovered, what is known, and what is not yet known. Everything that follows is logged against that record, so the timeline is reconstructable afterwards.

Step 2 — Contain (within hours)

Priority is stopping the harm, not explaining it. Depending on the incident: revoke or rotate credentials and tokens, disable the affected function or endpoint, roll back the change that caused it, or take the affected component offline. Containment is never delayed to protect appearances.

Step 3 — Assess (within 24 hours)

Establish which customers are affected, which categories of personal data and roughly how many records and data subjects are involved, whether data was read, altered or exfiltrated, and the likely consequences for the individuals concerned.

Step 4 — Notify the customer (within 48 hours)

Written notification to the customer's registered data protection contact, containing:

- the nature of the incident and when it was discovered;
- the categories and approximate number of data subjects and records concerned;
- the likely consequences;
- the measures already taken and those proposed;
- the name and contact details of the person who can answer further questions.

If some facts are not yet established, the notification is sent anyway, marked as provisional, and updated without further undue delay. **A partial notification within 48 hours is always preferred over a complete one that is late.**

Step 5 — Remediate and verify

Fix the root cause, not the symptom. Where the incident touched access control or customer separation, an automated regression test is added so the same failure cannot return unnoticed. The fix is verified before the incident is closed.

Step 6 — Report and learn (within 10 business days of closure)

The affected customer receives a written report: timeline, root cause, data affected, actions taken, structural measures and — where relevant — what the customer should do on its side. Where the lesson is general, the Security Statement or this procedure is updated.

4. Availability incidents

For S4 incidents the customer is informed as soon as the cause is known, with an expected restoration time and, where the outage falls in a shift change, a practical workaround: schedules exported to Excel or PDF remain usable offline, which is one of the reasons exports exist in every module.

5. Reporting an incident to us

If you believe data is exposed, or you find a security defect:

- Email **info@kaizenkanri.nl** with "SECURITY" in the subject line.
- Describe what you observed, the URL or screen, the approximate time, and the account used.
- Do not test further, do not attempt to access data that is not yours, and do not publish the finding before it is fixed.

Reports from customers, workers and independent researchers are welcome and are acknowledged within one business day. Good-faith reporters are never pursued; Kaizen Kanri would rather be told than discover it later.

6. Contacts

Purpose	Contact
Security incidents and breach reports	info@kaizenkanri.nl (subject: SECURITY)
Data protection matters, DPA, sub-processors	info@kaizenkanri.nl

Purpose	Contact
Customer's own notification contact	Recorded in Annex I of the Data Processing Agreement

7. Review

This procedure is reviewed at least once a year and after every S1 or S2 incident.

Kanriva™ and FlowCrew™ are trademarks of Kaizen Kanri.