MAELSTROM AI TRUST CENTRE

downpipes

Vendor Security and Assurance Pack

No-custody backup and disaster recovery for the Cloudflare data layer.

One document that answers a vendor security review: the architecture, the security posture, the control mappings, the shared-responsibility boundary, how support access works, and a pre-answered questionnaire. Free and public, with no contract, no NDA, and no login.

What does Maelstrom hold of your downpipes data?

Nothing.

No data. No keys. No tokens. The engine runs in your account, not ours.

No custody · Post-quantum hybrid · MIT offline reader · Fail-open licensing · ASVS 5.0 L1 and L2

VERSION	DATE	CLASSIFICATION
1.0	19 June 2026	Public
STATUS	**APPLIES TO**	**OWNER**
Current	downpipes	Maelstrom AI, security@maelstrom.au

Versioned in source control; the Trust Centre is the live source. Publisher: Maelstrom AI Pty Ltd ATF Maelstrom AI Holding Trust (ABN 61 633 823 792).

TRUST AT A GLANCE

The whole pack, in one scan

CUSTODY

Maelstrom holds none of your data, keys or tokens, in either posture.

See 03

RECOVERY

Restores with an MIT, offline, no-network reader. Two independent implementations.

See 04

POSTURE

ASVS 5.0 Levels 1 and 2, zero open gaps. Post-quantum hybrid seal. Hourly canary.

See 05

SCOPE

A supplier of self-hosted software, not a data processor or sub-processor. Provii is out of scope.

See 01

SOC 2 and ISO 27001 are on the roadmap and stated as such, not claimed. Verify any of the above yourself: the full ISMS is published ungated at maelstrom.au/trust, the offline reader is MIT-licensed, and the platform is source-available.

CONTENTS

Thirteen nodes on one chain

01

THE SHORT VERSION

Scope us out

downpipes is self-hosted software that runs inside your own Cloudflare account. Through downpipes, Maelstrom AI holds none of your data, none of your encryption keys, and none of your Cloudflare tokens, at any time. There is no Maelstrom-operated system that stores or processes your downpipes backups.

For vendor risk, the accurate classification of Maelstrom AI in respect of downpipes is a supplier of self-hosted software, not a data processor or a sub-processor. For downpipes we process no personal data on your behalf; the software does, inside your tenancy, under your control. A compromise of Maelstrom cannot expose your downpipes backups, because we cannot read them, and your recovery does not depend on Maelstrom continuing to exist.

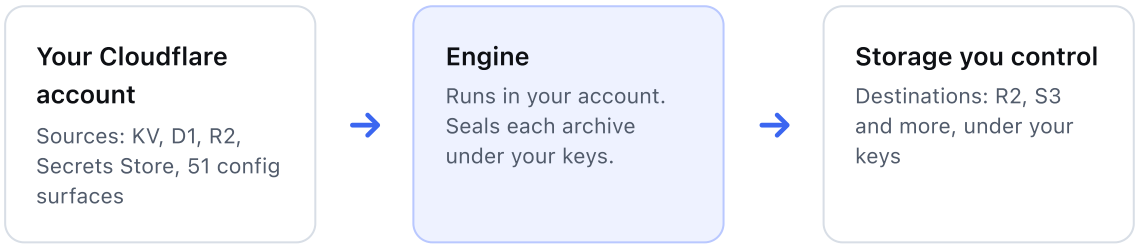
> Paste this into your risk register: *In respect of downpipes, Maelstrom AI is a supplier of self-hosted software, not a data processor or sub-processor for our data. It holds none of our data, keys or tokens; the software runs in our own Cloudflare account, under our keys. Maelstrom's other products are separate services, out of scope for this assessment.*

02

THE PRODUCT

What downpipes is, and how it runs

downpipes backs up Cloudflare Workers KV, D1, R2, Secrets Store and 51 Cloudflare configuration surfaces to storage you control, encrypted under keys only you hold. It has three parts: an **engine** (a Cloudflare Worker that runs in your account and writes encrypted archives to your destinations), a **console** (the management interface, also in your account), and an **offline reader** (a single open-source binary that restores an archive with no network and no vendor).



Restore runs the other way, with your keys, using the MIT offline reader. It needs no network and no vendor.

Maelstrom-operated and content-free: the control plane (a licence token and an optional beacon, fail-open) and the update channel (signed, read-only, no phone-home). Neither sees your data.

Figure 1. Data flow and trust boundary. Sources, engine and destinations are all in your account, under your keys.

03

CUSTODY

No custody, by construction

Keys are generated in your browser during a guided ceremony and are never transmitted. The break-glass key, the one that can decrypt everything, lives offline, with you. The engine seals each archive to public keys; the private keys it never holds. So Maelstrom cannot read your backups or decrypt your archives, and a subpoena served on Maelstrom yields none of your backup data, because we hold none of it.

The residual disclosure worth reading twice: in the default operational posture, an operational private key, capable of decryption, sits in your in-account engine so backups can run unattended. It is your key, in your engine, in your account. You can switch to a strict break-glass-only posture from the Keys screen; the trade-off is stated in the product and in the ISMS. Maelstrom holds no key of yours in either posture.

04

RECOVERY

Recovery does not depend on us

The archive format (downpipe/1.0) is a frozen, public, normative specification with a published conformance corpus. There are two independent implementations, the Go reader and the TypeScript engine, sharing no code, each proven to read what the other writes. The offline reader is MIT-licensed: a single Go binary, with no telemetry, no SDK, and no network dependency. If Maelstrom disappeared tomorrow, you would still restore from your archives, with your keys, using an open tool. For a backup product, that is the definition of no lock-in.

05

SECURITY POSTURE

What is verifiable today

Every property below is either enforced by cryptography or verifiable by you.

ASVS 5.0, Levels 1 and 2

Self-assessed with zero open gaps as of June 2026, including five follow-up remediations completed and re-verified. The full assessment is available on request, no NDA.

Post-quantum hybrid cryptography

X25519 with ML-KEM-1024 (FIPS 203) for key encapsulation; Ed25519 with ML-DSA-87 (FIPS 204) for signatures; AES-256-GCM for content; SHA-384 and HKDF-SHA-384. A break in either half alone does not break the seal.

Threat model and architecture

A written threat model, architecture and data-flow documentation, and a cryptographic bill of materials, all available on request.

Continuous integrity

An hourly canary flight proves byte-exact recovery across destinations; a hash-chained, tamper-evident audit log records gated actions, denials, role and configuration changes, and is exportable.

Access control

SSO via Cloudflare Access, WebAuthn passkeys, single-use recovery codes, and four-role RBAC with dual-control approvals. Standard in every edition, with no SSO surcharge.

06

CONTROL MAPPINGS

What downpipes evidences

A product does not make you compliant; that obligation stays with you. What downpipes does is prove the backup-and-recovery control the way an assessor wants to see it: verified on each run, dated, and exportable. Each mapping is published with its evidence at maelstrom.au/trust.

- **Essential Eight.** Regular Backups, Maturity Levels 1 to 3.
- **ISM.** ISM-1511, ISM-1515, ISM-1705 to 1708, ISM-1810 to 1814.
- **Australian regimes.** APRA CPS 234 and CPS 230, SOCI Act and CIRMP, Privacy Act and APP 11.
- **International.** DORA Articles 11 to 12 (segregated backups, defined RTO and RPO, integrity checks during recovery, at-least-annual restore testing); SEC 17a-4 (a complete, tamper-evident record); NIS2 (business continuity and tested recovery).

Maelstrom AI backs up its own Cloudflare estate with a production instance of downpipes. We dogfood it deliberately; the evidence is in the Trust Centre.

07

SHARED RESPONSIBILITY

Who controls what

Because downpipes runs in your account, some controls are yours. This is the boundary an assessor needs to see.

TABLE 1. SHARED-RESPONSIBILITY MATRIX.

CONTROL	MAELSTROM	CLOUDFLARE	YOU
downpipes software security	✓	–	–
Vendor control plane and update channel	✓	–	–
Operating the in-account engine and console	–	–	✓
Generating and safeguarding break-glass keys	–	–	✓
Destinations, retention and restore-test cadence	–	–	✓
Identity provider and operator access in your tenant	–	–	✓
Underlying edge compute and storage	–	✓	–

08

SUB-PROCESSORS

None in the data path

No third party, Maelstrom included, processes your backup data. downpipes adds no sub-processor, because no downpipes customer data is processed by or for Maelstrom. Maelstrom's own subservice organisations, supporting the control plane and update channel and not your data, are Cloudflare (compute, storage, access) and GitHub (source control and CI/CD). Both hold their own SOC 2 Type II and ISO 27001; we obtain and review those reports annually.

09

OPERATING PRACTICE

How support access works

> Paid support holds no standing access to your account. When you ask for help and grant access, that access is requested in the open and approved by you, read-only by default and scoped to the task, time-boxed and revocable by you at any time, and written to your audit log. Between engagements, the vendor holds nothing. Support operates within the no-custody model; it does not change it.

10

CERTIFICATIONS

What we hold, and what we do not

We do not currently hold SOC 2 or ISO 27001 certification. Both are on the roadmap; ask for current status and we will tell you the truth, including dates we are unsure of. Our ISMS is structured to ISO/IEC 27001:2022 and is published in full and ungated: the policies, the Statement of Applicability, the risk register, and the data protection assessments.

Certification is demand-gated: for a no-custody, self-hosted product there is essentially no vendor-held system to attest, and the architecture is a stronger answer than a report. A third-party penetration test report once completed, and any certificate once held, are available to a serious evaluator under a mutual NDA, at no charge. What we will not claim: there is no Essential Eight certification, for anyone, and IRAP assessors assess systems, not products.

11

LEGAL AND CONTRACTUAL

The DPA, and what the paid tiers add

downpipes is free to run. The paid tiers buy a relationship, never the software.

- **Data Processing Agreement.** A signable DPA is published at maelstrom.au/trust. Because downpipes is no-custody, most of a standard DPA is satisfied by the architecture, and the document says so honestly.

- **Enterprise adds** (priced separately, see downpipes.io/pricing): a support response SLA, a named contact, a counter-signed DPA on our standard paper, your own security questionnaire completed under our signature, and a set number of vendor-assessment calls each year.
- **Custom covers** contracts on your paper, bespoke security and liability terms, formal audit support, deployment and recovery services, and 24/7 critical-incident response.

12

SAMPLE QUESTIONNAIRE

The common questions, pre-answered

A full CAIQ or SIG-lite is completed for Enterprise customers; this sample lets you pre-clear the basics today.

Where is customer data stored?
In your own Cloudflare account, and the destinations you choose. Maelstrom stores none of it.

Who can access customer data?
Only you. Maelstrom cannot decrypt your archives.

How is access controlled?
SSO, passkeys, four-role RBAC, dual-control approvals, and a hash-chained audit log.

Do you test recovery?
Yes. An hourly canary, plus signed restore-test drills.

Is the software auditable?
Yes. The engine, console and control plane are source-available under the Elastic License 2.0; the offline reader is MIT-licensed.

Is data encrypted at rest and in transit?
Yes. Archives are sealed with post-quantum hybrid encryption under your keys; transport is over TLS.

Do you use sub-processors for customer data?
No.

Do you run a vulnerability disclosure process?
Yes. security@maelstrom.au and /.well-known/security.txt, with CVSS-based remediation targets (Critical 48 hours, High 7 days, Medium 30 days, Low 90 days).

What is your breach-notification commitment?
Because Maelstrom holds none of your downpipes backup data, a Maelstrom incident cannot breach your backups. Control-plane or update-channel incidents are notified under the Enterprise agreement.

What happens if we stop paying, or you disappear?
Nothing to your backups or restores. Licensing is fail-open; the product keeps running as Community, and recovery uses the open offline reader.

13

NEXT

Where to go next

Everything here is free and verifiable, with a live source for each.

- The full ISMS, ungated, covering Maelstrom AI and Provii as well as downpipes: maelstrom.au/trust
- The product, source and architecture: downpipes.io
- Pricing, and what Enterprise adds: downpipes.io/pricing
- Security contact and disclosure: security@maelstrom.au
- To request the full ASVS assessment or threat model, or to set up an NDA for sensitive documents: maelstrom.au/contact

downpipes

Nothing.

That is what we hold of your downpipes data. The rest of the chain continues, versioned and live, at the Trust Centre.

DOCUMENT	downpipes Vendor Security and Assurance Pack
VERSION	1.0 · 19 June 2026 · Public · Current
PUBLISHER	Maelstrom AI Pty Ltd ATF Maelstrom AI Holding Trust (ABN 61 633 823 792)
CONTACT	security@maelstrom.au · maelstrom.au/trust

This document is published and versioned at the Maelstrom AI Trust Centre. Printed copies are uncontrolled; verify the current version online.