Malcolm Central – Security, Integrations & Compliance Overview

Document purpose: This page summarises the security, availability and operational controls of the Malcolm platform, and the integrations it supports. It is intended to give clients and their security reviewers a clear, honest picture of how Malcolm protects data. More detailed assurance material — including a per-client security & compliance pack and a penetration-testing executive summary — is available on request under confidentiality (see Further Assurance below).

Document status: This page is not a certification, audit report or legal advice; it describes controls aligned with the SOC 2 Trust Services Criteria.

Hicaliber Pty Ltd
Prepared by: Hicaliber
Version: 1.0
Last updated: 22 July 2026

---

1. What Malcolm Central Is

- **A real-estate data-integration (middleware) platform.** It connects the systems an agency already uses — PropTech CRMs, sales and campaign tools, payment/credit providers, portals, reporting tools and websites — and keeps data in sync between them.
- **What it is not:** a credit provider, a KYC system, or a store of identity documents.
- **What it moves:** operational business data — listings, contacts, campaign and request data — and only between systems the client authorises.

---

2. Supported Integrations

Only explicitly configured integrations are active for a client. Each vendor can access only the endpoints its integration needs.

PropTech CRMs

- Rex Software
- Reapit (AgentBox)

- VaultRE
- Box & Dice
- Property Suite (CSV ingestion)
- MultiArray
- *On the roadmap: PropertyTree, LockedOn, Property Me*

Sales & Campaign

- Realtair
- Real Time Agent
- CampaignTrack
- AuctionsLive
- Property Credit
- SaleFunder
- Rello
- Realty Assist
- REA Reviews
- REA
- Domain
- OpenLot
- Proptrack
- PriceFinder
- Diakrit
- Google Business Profile

CRM & Marketing

- HubSpot
- Sugar CRM
- Salesforce CRM
- Salesforce Marketing Cloud
- Airtable
- Monday.com

Communications & Web

- Aircall

- 3CX
- ConnexOne
- Slack
- Mailgun (email)
- SendGrid (email — being phased out)
- Twilio (SMS)
- WordPress

---

3. Security Architecture at a Glance

- **Everything runs on AWS**, provisioned as infrastructure-as-code.
- **Edge protection (all new deployments):** traffic enters through **Amazon CloudFront** with an **AWS WAF** — TLS 1.2+, per-IP rate limiting, OWASP-aligned managed protections, IP-reputation filtering and bot mitigation. Automated, 24/7.
- **Load-balanced application tier:** requests pass through an AWS Application Load Balancer to the application, which runs in Docker containers. On new deployments the application servers are not directly reachable from the internet.
- **Per-client isolation** — depending on the plan, a client runs in a dedicated AWS account or as an isolated tenant on a shared server; in both cases with its own database, credentials and storage. Separate development, staging and production environments.
- **Databases are never internet-exposed** — reachable only from the application tier.
- **Encryption everywhere:** TLS in transit; AES-256 at rest (S3 and storage volumes). Customer-managed keys available on request.
- **Australian data residency:** AWS Sydney (ap-southeast-2), confirmed per deployment.

Deployment generations. The architecture above is the standard for all new Malcolm deployments. Some earlier deployments run a previous-generation hardened configuration and are progressively upgraded; the exact configuration of a given deployment is confirmed in its architecture pack (section 13).

---

4. Data Handling & Privacy

- **Data minimisation.** We store only what is needed to deliver the configured service — typically listings, agency/office data, contacts and enquiries, sync histories and operational logs.
- **No identity documents.** Malcolm Central does not receive or store identity ("100-point") documents or credit-decision documents; those remain with the client's downstream provider.
- **No secondary use.** No direct marketing, no sale of data, no model training, no unauthorised analytics.
- **Retention.** Defined per client deployment (period, trigger, responsible party, automated vs requested). Infrastructure level: backups kept ~1 month; operational logs ~2–4 weeks. Scheduled automated purge lifecycles can be implemented as a scoped engagement.

---

5. Access Control

- **Role-based access control** in the platform — enforced server-side on a least-privilege basis and adjustable per client. Standard roles:
  - Super-admin
  - Admin
  - State team
  - Office team
  - Customer
  - Compliance manager
  - Reports manager
  - Accounting manager
  - Fund provider
- **MFA everywhere:** AWS and all major internal systems; centralised identity via Google Workspace.
- **Restricted production access:** limited to the lead engineer and assigned project team; administrative access only from approved locations; structured onboarding/offboarding.
- **Least-privilege integrations:** minimum vendor scopes per configuration — including **read-only provisioning** where a use case (such as a payment/credit integration) does not need write access to the client's CRM.

HICALIBER

6. Monitoring, Alerting & Availability

- **Continuous automated protection:** the edge WAF inspects, rate-limits and blocks malicious traffic around the clock, independent of staffing.
- **Real-time alerting:** infrastructure alarms (CPU, memory, disk) and application heartbeat/error alerts notify the engineering team immediately.
- **Audit logging** of key application activity; blocked-request logs retained for investigation.
- **Staffed 24/7 monitoring** and enhanced containment SLAs are available as a managed-service engagement for enterprise clients.

---

7. Backups & Disaster Recovery

- **Automated daily backups** of every production environment, retained ~1 month in a dedicated backup vault.
- **Restores are periodically tested** — recovery is proven, not assumed.
- **Typical recovery targets:** RPO ~1 day · RTO ~1–3 hours (scenario-dependent).

---

8. Secure Development & Deployment

- **Pull-request review** for every change.
- **CI/CD pipeline** with automated static analysis, code-style enforcement and automated tests; deploys through sandbox before production.
- **Dependency security advisories** enforced automatically in the build.
- **Immutable, versioned deployments:** container images from a private registry; infrastructure provisioned as reviewable code.

---

9. Security Testing

- **Regular, on-demand penetration assessment** of the shared product codebase — authentication, authorisation, injection, XSS, SSRF, path traversal, file uploads, privilege escalation and API error handling; findings scored against CVSS v3.1.

- **Most recent assessment (February 2026): no critical or high-severity vulnerabilities.** The small number of medium/low findings were remediated and verified; no data exposure or compromise.
- **Redacted executive summary** available to clients on request, under confidentiality.
- **Client-directed testing welcome:** a non-production environment can be provided — as we have done for enterprise real-estate clients running their own security review.

---

10. Cyber Incident & Breach Remediation Process

A defined, repeatable process aligned with Australian Cyber Security Centre (cyber.gov.au) guidance. All incidents are logged and tracked in our service-management system.

1. **Detect & report** — WAF blocks, infrastructure alarms, application alerts, log review, client/vendor reports.
2. **Triage & classify** — confirmed vs suspected; severity assigned; engineering leads own the response.
3. **Contain** — isolate components, revoke/rotate credentials and keys, tighten edge rules, preserve evidence.
4. **Eradicate & recover** — remove the root cause, patch, restore from verified backups, validate data integrity.
5. **Notify & communicate** — clients notified without undue delay. Under the **Notifiable Data Breaches (NDB) scheme**, the data controller notifies the **OAIC** and affected individuals; where Hicaliber is data processor, we support the investigation and notify the client promptly. Roles confirmed in each agreement.
6. **Review & improve** — root-cause analysis and corrective actions tracked to completion.

Severity levels and indicative response:

- **Critical** — confirmed data exposure or active compromise; response: immediate (contain first).
- **High** — suspected breach or authentication failure; response: same business day.
- **Medium** — isolated defect with limited exposure; response: prioritised in the current cycle.
- **Low** — minor hardening issue, no exposure; response: scheduled.

---

11. Compliance Position & Certification Roadmap

- **Not currently SOC 2 (Type I/II) audited or ISO 27001 certified** — we state this plainly rather than imply a certification we do not hold.
- **Controls aligned with the SOC 2 Trust Services Criteria** (security, availability, confidentiality); a **formal SOC 2 certification pathway is planned**.
- **Core sub-processors are independently certified:**
  - **AWS** — hosting, CDN & WAF (SOC 1 / 2 / 3)
  - **Google Workspace** — identity & collaboration (SOC 2)
  - **Mailgun / Twilio** — email / SMS; SendGrid being phased out (SOC 2)
  - **Airtable** — reporting, where used (SOC 2)
- **KYC / credit-scoring providers** are engaged by the downstream provider — not by Malcolm Central — and hold their own attestations. A full sub-processor inventory is available on request.

---

12. Frequently Asked Security Questions

Does Malcolm Central store our data, or is it purely transient?

Not purely transient — it stores the operational data needed to sync systems (listings, contacts, enquiries, sync metadata), under data minimisation. No identity documents.

Is our data hosted in Australia?

Yes for Australian clients — AWS Sydney (ap-southeast-2), confirmed per deployment including backups.

Can the integration run read-only on our CRM?

Yes, where the use case allows it. Payment/credit-style integrations can be provisioned without write access or directory-level scopes. Scope mapping is agreed at onboarding.

How is traffic between systems secured?

HTTPS/TLS end-to-end, per-vendor authentication (API keys, tokens, OAuth) and webhook secrets; new deployments additionally place an edge WAF in front of all inbound traffic.

What happens if there is a data breach?

The process in section 10: contain, remediate, notify affected clients without undue delay, support NDB/OAIC obligations.

Are you SOC 2 certified? Can we see a pen-test report?

Not certified (section 11). A redacted pen-test executive summary is available under confidentiality; clients can also test a non-production environment themselves.

How do you monitor with a small team?

Edge protection and alerting are automated and continuous; a staffed 24/7 arrangement is available as a managed-service engagement.

---

13. Further Assurance Available on Request

1. **Malcolm Central — Security & Compliance Overview** — the detailed per-client due-diligence document.
2. **Penetration Testing Executive Summary** — redacted results of the most recent assessment (under confidentiality).
3. **Per-deployment Architecture Pack** — architecture, access and tech-stack documentation for your deployment, plus a non-production environment for your own penetration testing.
4. **Control evidence** — backup/restore history, alarm configuration, access reviews, incident-ticket examples, sub-processor assurances.

---

14. Security Contact

- **Primary technical & incident contact:** Nikita Alekseev, Head of Engineering — nikita.alekseev@hicaliber.com.au
- **Escalation / operations:** Amy Smith, Head of Operations — amy.smith@hicaliber.com.au