# Data Centre and Security Measures (DCSM)

BidClarity Ltd · Version 1.1 · Effective 17 July 2026

## 1. Overview

This Data Centre and Security Measures document ("DCSM") describes the technical and organisational measures BidClarity applies to protect Customer data processed on the BidClarity platform. It is incorporated into the DPA by reference.

## 2. Hosting and data residency

The BidClarity platform is hosted on Cloudflare (edge + Workers) and Supabase (Postgres, storage) in the United Kingdom and European Economic Area. Customer data is stored at rest exclusively in UK/EEA regions.

## 3. Access control

Role-based access control at the application layer with Postgres row-level security enforcing tenant isolation. Employee production access is limited to a named on-call rota, requires SSO with hardware-key MFA, and is audit-logged.

## 4. Encryption

TLS 1.2+ in transit for all endpoints, HSTS enforced. AES-256 encryption at rest for database volumes, object storage, and backups. Per-user provider credentials (e.g. SharePoint connection keys) are additionally encrypted with AES-256-GCM at the application layer using a Lovable-managed key that is never exposed to Customer databases.

## 5. Network security

All traffic terminates at Cloudflare with DDoS protection, WAF, and rate limiting. Origin services are private and reachable only via authenticated worker requests. No inbound SSH to production.

## 6. Application security

Secure SDLC with mandatory code review, dependency scanning, and automated security tests on every deployment. Least-privilege service accounts, secrets stored in a managed secret store, never in source control.

## 7. Logging and monitoring

Application, authentication, and admin actions are logged with timestamps and actor identity. Logs are retained for 90 days in a tamper-evident store. 24/7 alerting on anomalous access patterns and error-rate spikes.

## 8. Backups and recovery

Encrypted point-in-time Postgres backups with a 7-day recovery window; daily snapshots retained for 30 days. RPO 15 minutes, RTO 4 hours. Recovery is tested at least twice a year.

## 9. Personnel

All personnel undergo background checks and annual security training. Access is revoked within one business day of role change or departure.

## 10. Sub-processors

Current sub-processors: Cloudflare (hosting, CDN, WAF), Supabase (managed Postgres, storage, auth), Google Cloud (AI Gateway inference, EU region), Resend (transactional email). Full list and updates available on request.

## 11. Incident response

24/7 on-call rota with a documented incident-response playbook. Customer-affecting incidents trigger notification within 48 hours per the DPA, with root-cause analysis provided within 10 business days.

## 12. Certifications and audits

BidClarity aligns its control set to ISO 27001 and SOC 2 Type II. A summary letter of the most recent penetration test is available under NDA to Enterprise customers.

Questions: privacy@bidclarity.co.uk · BidClarity Ltd, London, United Kingdom