



SERVICE DATASHEET

Data SECURITY

Threat modelling, access control, encryption, testing, monitoring and governance, designed into the build.

Security work that starts after a system is live is always more expensive and less effective. We model the threats before the architecture is fixed, then verify the result with testing rather than assurances. Protection is part of the build, not a layer added at the end.



Security architecture

Threat modelling, trust boundaries and controls agreed before development begins.



Encryption and keys

Data protected in transit and at rest, with managed keys and certificate lifecycles.



Monitoring and response

Central logging, alerting, audit trails and a rehearsed incident response process.



Identity and access

Role based permissions, multi factor authentication and segregation of duties.



Testing and remediation

Vulnerability assessment, penetration testing, code review and a prioritised fix plan.



Governance and continuity

POPIA and GDPR readiness, retention policy, backup and tested disaster recovery.

ASSURANCE

Findings fixed before release rather than logged for later · The maker of a transaction cannot be its checker or its payer · Every decision traceable to a user, a rule and a timestamp · Recovery designed and then actually tested

WHO IT IS FOR

Regulated buyers · Financial services · Health risk administrators · Public sector · Any business holding personal data