1. Introduction

Catapult Smallprint Pty Ltd are committed to protecting the confidentiality, integrity and availability of the data entrusted to us by our customers and users.

This Data Security Statement explains, at a high level, the technical and organisational measures we use to protect customer data across the Vasto and Catapult platforms.

This document is intended to support customer assurance, procurement, privacy reviews, security questionnaires and general enquiries about how data is protected. It should be read together with our Privacy Policy, customer agreements, platform terms, AI Policy and any product-specific documentation or contractual commitments.

2. Scope

This statement applies to the Vasto and Catapult platforms, including the systems, databases, storage, integrations, support processes and operational activities used to provide those services.

This statement applies to customer data, learner data, student data, administrator data, course and enrolment data, assessment-related data, support information, platform records and related business information processed by Vasto and Catapult.

This statement does not cover systems, vendors, integrations or customer-managed environments that are outside Catapult's operational control, except where expressly stated.

3. Certification and assurance status

Vasto and Catapult are not currently certified to ISO/IEC 27001 and do not currently hold SOC 2 reports.

Our parent company, AdNeo Pty Ltd, is developing and improving group-wide security documentation, policies and operating practices to support stronger and more consistent security governance across its platforms.

Where a customer requires formal certification, independent audit reports, penetration test summaries or detailed security documentation, this should be raised with AdNeo so that the current status and available evidence can be confirmed.

4. Hosting and data location

The Vasto and Catapult platforms are hosted using Amazon Web Services in the Sydney, Australia region.

Customer production data for Vasto and Catapult is stored in Australia unless otherwise agreed in writing or required by a customer-authorised integration, support process, service provider or legal obligation.

Some service providers, support tools, analytics tools, communication tools, monitoring tools or integrations may involve access from, processing in, or support from locations outside Australia. Where this occurs, Catapult seeks to ensure that appropriate contractual, privacy and security controls are applied.

5. Security governance

Catapult manages security through a combination of policies, technical controls, access management, monitoring, staff responsibilities, incident response processes and platform-specific operational procedures.

Security responsibilities are assigned to appropriate business and technology roles. Staff and contractors are expected to follow Catapult policies relating to acceptable use, information security, data protection, AI use, access control, incident reporting and confidentiality.

Security risks, exceptions and improvements should be reviewed and addressed based on business impact, customer impact, likelihood and available controls.

6. Data protection approach

Catapult applies a layered approach to data protection. Controls may include:

- role-based access controls;
- least-privilege access principles;
- authentication and password controls;
- multi-factor authentication for privileged access where supported and appropriate;
- segregation between customer accounts or tenants through application and database controls;
- encryption in transit;
- encryption at rest where supported and configured;
- logging and monitoring of relevant system activity;
- backups and recovery processes;
- vulnerability and patch management;
- secure development and change management processes; and
- incident response and breach assessment processes.

7. Access control

Access to production systems and customer data is limited to authorised personnel who require access to perform their role.

Access is granted based on business need and should be removed or updated when a person changes role, no longer requires access, or leaves the organisation.

Privileged access is restricted to authorised personnel. Shared accounts should be avoided where individual accounts can reasonably be used.

Catapult aims to maintain clear records of access, approvals and changes to access for key systems.

8. Authentication and user security

Users are responsible for maintaining the confidentiality of their login credentials and for using the security controls made available through the relevant platform.

Administrative and privileged users should use strong authentication practices, including multi-factor authentication where available.

Password controls, session management and authentication requirements may differ by platform, user role and customer configuration.

9. Encryption

Catapult uses encryption to protect data where appropriate and technically supported.

Data transmitted over public networks is protected using encrypted connections such as HTTPS/TLS.

Data at rest, including databases, storage volumes, object storage and backups, should be encrypted where supported and configured for the relevant platform and AWS service.

Encryption controls may vary by platform, legacy system, integration and storage type. Where a customer requires specific encryption commitments, these should be confirmed contractually.

10. Backups, availability and recovery

Vasto and Catapult use backup and recovery processes appropriate to the services being provided.

Backups are used to support recovery from data loss, system failure, operational error or other disruptive events.

Backup frequency, retention periods and recovery testing may vary by platform and system component. Platform-specific details are set out in the schedules below or may be provided on request where available.

Catapult aims to maintain recovery processes that support continuity of critical services, while recognising that recovery time and recovery point outcomes depend on the nature and severity of the incident.

11. Monitoring and logging

Catapult uses system, application, infrastructure and security logs to support operation, troubleshooting, security monitoring and incident investigation.

Monitoring may include application health, infrastructure health, availability, errors, suspicious activity, authentication activity, access events, performance issues and operational alerts.

Logs are accessed by authorised personnel for legitimate operational, security, compliance and support purposes.

12. Vulnerability management and patching

Catapult seeks to identify, assess and remediate vulnerabilities affecting its platforms, infrastructure, dependencies and applications.

Vulnerability management activities may include vulnerability scanning, dependency review, patching, code review, security testing, third-party notifications, customer reports and investigation of reported issues.

Findings are prioritised based on severity, exploitability, affected systems, customer impact and business risk.

Where a vulnerability cannot be immediately resolved, Catapult may apply compensating controls, risk acceptance or staged remediation based on the nature of the issue.

13. Secure development and change management

Catapult uses development and change management practices to reduce the risk of unplanned outages, security weaknesses and data integrity issues.

These practices may include source control, pull requests or peer review, testing in non-production environments, deployment controls, rollback planning, separation between development and production environments, and post-release verification.

Production changes should be performed by authorised personnel and should be assessed for operational and security impact before release.

14. Testing and non-production environments

Where possible, testing should be performed in non-production environments using synthetic, anonymised or de-identified data.

Production data should not be copied into local, development or testing environments unless specifically authorised and protected by appropriate safeguards.

Where production data must be used for support, debugging, migration, audit or investigation purposes, access should be limited, justified and removed once no longer required.

15. Incident response and data breach management

Catapult maintains processes for responding to suspected or confirmed security incidents.

If a security incident occurs, Catapult will seek to identify, contain, investigate, remediate and document the incident. Where personal information is involved, Catapult will assess whether the incident is likely to result in serious harm and whether notification is required under applicable privacy laws or customer agreements.

Where required, Catapult will notify affected customers, individuals, regulators or other parties, or assist the relevant customer to do so where the customer is responsible for notification.

16. Third-party providers and subprocessors

Catapult uses third-party providers to support hosting, infrastructure, monitoring, communications, payments, support, development, analytics, security and other business functions.

Third-party providers are selected and managed based on the nature of the service, the type of data involved, business criticality and security risk.

Where third parties process customer or personal information on behalf of Catapult , Catapult seeks to ensure that appropriate contractual, privacy and security obligations are in place.

17. Artificial intelligence and automation

Catapult may use approved artificial intelligence, machine learning, automation or analytics tools to support business operations, platform functionality, support, security, reporting and product improvement.

Use of AI tools is governed by AdNeo's AI Policy and related data protection requirements.

Personnel must not intentionally input confidential customer data, personal information or regulated data into unapproved AI tools.

Where a platform-specific AI feature is made available to a customer, additional product documentation, terms or notices may apply.

18. Customer responsibilities

Customers play an important role in protecting their own data and users.

Customers are responsible for:

- managing their authorised users and administrators;
- promptly removing access that is no longer required;
- using strong passwords and multi-factor authentication where available;
- ensuring users understand their privacy and security obligations;
- configuring platform permissions appropriately;
- protecting exported reports and downloaded data;
- ensuring third-party integrations are authorised and appropriate;
- notifying Catapult promptly of suspected security issues or unauthorised access; and
- complying with applicable privacy, education, employment, training and records obligations.

19. Product schedule — Vasto

Area	Current statement
Platform	Vasto
Primary hosting location	Amazon Web Services, Sydney, Australia
Data residency	Customer production data is stored in Australia unless otherwise agreed or required for authorised integrations/support processes
Certification status	Not currently ISO/IEC 27001 certified; no current SOC 2 report
Primary data types	Student, learner, enrolment, course, assessment, reporting, support and administrative data
Access model	Role-based platform access and internal administrative access controls
Encryption in transit	HTTPS/TLS should be used for web traffic and supported integrations
Encryption at rest	To be confirmed for all databases, storage, volumes and backups before publication
Backups	Backup frequency, retention and restore testing to be confirmed before publication
Monitoring	Platform and infrastructure monitoring to be confirmed before publication
Vulnerability management	Current scanning, patching and testing approach to be confirmed before publication
Key subprocessors	To be confirmed before publication
AI-enabled processing	To be confirmed before publication

20. Product schedule — Catapult

Area	Current statement
Platform	Catapult
Primary hosting location	Amazon Web Services, Sydney, Australia
Data residency	Customer production data is stored in Australia unless otherwise agreed or required for authorised integrations/support processes
Certification status	Not currently ISO/IEC 27001 certified; no current SOC 2 report
Primary data types	Learning, course, enrolment, student, assessment, submission, communication, reporting, support and administrative data
Access model	Role-based platform access and internal administrative access controls
Encryption in transit	HTTPS/TLS should be used for web traffic and supported integrations
Encryption at rest	To be confirmed for all databases, storage, volumes and backups before publication
Backups	Backup frequency, retention and restore testing to be confirmed before publication
Monitoring	Platform and infrastructure monitoring to be confirmed before publication
Vulnerability management	Current scanning, patching and testing approach to be confirmed before publication
Key subprocessors	To be confirmed before publication
AI-enabled processing	To be confirmed before publication

21. Changes to this statement

Catapult may update this Data Security Statement from time to time to reflect changes in platforms, systems, controls, vendors, certifications, legal requirements or business operations.

The current version will be made available on request via Catapult and Vasto websites.