

Ready STA Security Processes

June 2026

A large, solid green shape that starts as a thin line on the left and expands diagonally upwards to the right, filling the bottom half of the page.



Table of Contents

1. INTRODUCTION	4
2. SECURITY AND COMPLIANCE	4
3. SHARED SECURITY RESPONSIBILITY MODEL	4
3.1 Infrastructure	5
3.2 Data Sovereignty	5
3.3 Data Ownership	5
4. PERSONNEL SECURITY	5
5. IDENTITY AND ACCESS MANAGEMENT	6
6. STANDARD OPERATING ENVIRONMENTS	6
7. PATCH MANAGEMENT	6
8. SOFTWARE DEVELOPMENT	7
9. DATABASE SYSTEMS	7
10. NETWORK SECURITY	7
11. CRYPTOGRAPHY	8
12. LOGGING AND MONITORING	8
13. PENETRATION TESTING	8
14. BACKUP MANAGEMENT	9
15. DATA RETENTION	9



16.	BUSINESS CONTINUITY	9
17.	INCIDENT MANAGEMENT	10
18.	THIRD PARTY SUPPLIER MANAGEMENT	10
19.	CONTACTS	11
20.	CLASSIFICATION	11
21.	DOCUMENT MANAGEMENT	11



1. Introduction

Ready STA provides Australia's State & Territory Governments with highly customised, purpose-built technology to deliver and manage complex apprenticeship programs – at scale. Making sure your data is secure and protecting it is one of ReadyTech's most important responsibilities. We're committed to being transparent about our security practices and helping you understand our approach.

2. Security and Compliance

ReadyTech has established an industry-leading security program, dedicated to ensuring customers have the highest confidence in our custodianship of their data. Our Information Security Management System (ISMS) is aligned to the ISO 27000 standards and is regularly audited and assessed by third parties.

Our ISO 27001:2022 certificate is available on the JAS-ANZ register: <https://register.jasanz.org/certified-organisations> (search "ReadyTech"). Or, on the ReadyTech website: <https://readytech.io/security-and-compliance>

3. Shared Security Responsibility Model

ReadyTech strives to protect the confidentiality, integrity and availability of all critical information and stored customer data.

While we manage security of the application, security in the application is the responsibility of the customer. Ready STA is provided as software-as-a-service, i.e., a fully functioning modern web application. ReadyTech is responsible for procuring, configuring, monitoring and maintaining all aspects of the computing environment, from the servers to the application. ReadyTech utilises Amazon Web Services (AWS), which is the world leading provider of cloud infrastructure. AWS physical and technical security practices are outlined in its whitepaper at <https://docs.aws.amazon.com/pdfs/whitepapers/latest/aws-overview/aws-overview.pdf#Security%20and%20compliance>

The customer is responsible for managing the access of their authorised users, password policies and configuring roles and permissions within the application itself.



Identity
Data/Content
Application
Operating System
Virtualisation
Network
Infrastructure
Physical

	Customer Responsibility	Security in the application
	ReadyTech Responsibility	Security of the application
	AWS Responsibility	Security of the cloud

3.1 Infrastructure

Ready STA is hosted in the public cloud with AWS. AWS provides state-of-the-art data centres and a world-leading compliance program. AWS operates, manages and controls the components from the network layer down to the physical security of the facilities in which Ready STA operates. AWS manages the network devices but ReadyTech is responsible for secure network configuration.

3.2 Data Sovereignty

Ready STA only uses the AWS Sydney region to ensure data is stored and processed within Australia. AWS currently offer 3 different data centres or "availability zones" (AZs) in the Sydney region. Data and services are replicated across zones for high availability.

3.3 Data Ownership

The customer always owns their data. ReadyTech collects and processes data on behalf of the customer as required to provide and support the platform, as further detailed in the Privacy Policy: readytech.io/privacy

4. Personnel Security

All ReadyTech staff undergo screening checks before employment including reference, qualification and police checks. Security awareness training is provided at initiation and continuously throughout the year. Staff with privileged access to systems or data receive additional job-specific training on privacy and security. Personnel requiring access to production systems or customer data are required to have undergone appropriate security clearances.



ReadyTech has appointed a Head of Security Operations who is responsible for the performance of the ISMS. All staff have security responsibilities assigned as part of their roles.

5. Identity and Access Management

Ready STA provides out of the box functionality to support secure access control for customers:

- Role-Based Access Control (RBAC) for configurable, granular provision of permissions and functionality to users.
- Enforced password complexity and expiration.
- Multi factor authentication (MFA).
- CAPTCHAs to prevent brute force attacks.

Access for ReadyTech staff to the application and infrastructure is provided on a least necessary privilege basis, with technical controls limiting access to approved staff, on compliant corporate devices validated with MFA. All staff devices, including laptops and mobile devices are centrally managed in the device management system to ensure they meet ReadyTech standards, which includes device encryption, password policies, malware control and time limited screen locking.

6. Standard Operating Environments

ReadyTech uses a documented Standard Operating Environment for all servers. The servers are provisioned through code and all change to the environment goes through ReadyTech secure programming practices.

7. Patch Management

Operating systems automatically apply security updates daily. Application vulnerabilities are identified through automated systems. The patching and upgrade of software components is incorporated into regular software development procedures and release schedules.

Critical issues and security patches may necessitate an out-of-cycle release, but these are processed through standard change management workflows.



8. Software Development

ReadyTech uses a Secure By Design approach in our Software Development Life Cycle. Security is considered in the design, development and testing of our software. We use a series of software development environments including development, staging and production. Software is only able to progress to the next environment after it passes all the checks at each level including mandatory internal peer code review, static code analysis, automated unit and integration testing, manual QA and UAT.

Access to release branches in the code version repository is strictly limited. ReadyTech use static code analysis tools to identify known vulnerabilities in developed code, conducted as part of the automated build pipeline.

ReadyTech web applications are developed using security best practice. All developers are trained to be aware of OWASP security guidelines. Database queries are parameterised. Application inputs and outputs are properly sanitised and encoded. Errors and exceptions are logged and monitored. User authentication passwords held within the database are stored salted and hashed.

9. Database Systems

Each customer uses a logically isolated database. Databases are securely provisioned with unique credentials per customer ensuring secure data partitioning. All use and administration of the database is through the web application frameworks minimising any exposure through direct database access. Database administrator accounts are only used to provision less privileged accounts for system use.

The network is designed to restrict access to the database to the fewest necessary systems. All database data is encrypted at rest using AES-256 with secure key management procedures.

Production, test and development environments are strictly separated on both the database and application server basis.

10. Network Security

ReadyTech divides its systems into separate networks (AWS VPCs) to better protect more sensitive data. Systems supporting testing and development activities are hosted on a separate network from production systems. Customer data is only permitted to exist in the production and staging networks.

Network access to the production environment from open, public networks (the internet) is restricted. Only required network protocols and ports are exposed to minimise the potential attack surface for malicious actors. Changes to the production network configuration are restricted to authorised personnel and all changes logged. ReadyTech uses an Infrastructure as Code approach to the network



configuration which uses versioned repositories and is deployed through automations to avoid potential misconfiguration.

11. Cryptography

Data at rest, and in transit, is only encrypted with ASD Approved Cryptographic Algorithms (AACAs) and ASD Approved Cryptographic Protocols (AACP).

Transport Layer Security (TLS) is used for all public network connections with a modern security policy meeting an SSL Labs A rating. The preferred server negotiated connection will be on TLS 1.3 with Elliptic Curve Diffie-Helman session keys and perfect forward secrecy. SSLv3, TLSv1.0 and TLSv1.1 are disabled. HTTP Strict Transport Security (HSTS) ensures that a TLS connection is always used.

AWS S3 is used for storage of documents and other unstructured data. S3 buckets are securely configured, objects are private and encrypted at rest using AES-256. Access to S3 objects exposed through the application, for authorised users, is provided through time limited (default 60 minutes) URLs.

Structured data stored in AWS RDS is encrypted at rest using AES-256.

12. Logging and Monitoring

Site uptime, host and application performance are monitored by independent third-party services with operational alerting and response procedures in place. Regular governance meetings and performance review ensure that the ongoing performance and availability targets are met.

ReadyTech uses Host Intrusion Detection, Network Intrusion Detection and Cloud Security Posture Management systems. Alerts are centrally monitored and acted upon by responsible teams.

13. Penetration Testing

ReadyTech conducts application penetration testing through an internal security function as part of its ongoing security assurance program. Penetration testing is performed regularly against the Ready STA application, with results reviewed by management and tracked through to remediation. Identified findings are assessed, prioritised, and resolved in accordance with ReadyTech's risk and vulnerability management processes.



Customers wishing to conduct their own penetration testing of the Ready STA application must obtain prior written permission from ReadyTech before commencing any testing activities.

14. Backup Management

The database operates on the AWS RDS service. Transaction log backups offer a Recovery Point Objective (RPO) of 5 minutes. In the event of a database service failure requiring recovery, the Recovery Time Objective (RTO) is approximately four hours.

Complete logical backups of the database are stored in S3 daily, offering 99.999999999% durability. Access to the logical backups is available to the customer if they would like to maintain external backups.

15. Data Retention

Data is retained within the system for the life of the contract. At contract termination, data is returned to the customer and permanently destroyed according to standard operating procedures. Data will be made available in standard, documented formats.

Database backups are retained for 12 months and deleted by automated lifecycle policies.

Data collected to support the delivery of the service, including system event and access logs will be retained for 7 years in accordance with the National Archives of Australia's Administrative Functions Disposal Authority Express Version 2 publication.

16. Business Continuity

The concepts of business continuity and disaster recovery are integrated into our design and architecture of highly available systems in the public cloud. Failure is routinely expected, planned for, tested and managed with automated systems and redundancy.

Resilience and scalability are addressed on AWS through:

- Running multiple EC2 instances in multiple Availability Zones (distinct locations that are engineered to be insulated from each other)
- Elastic Load Balancing across multiple Availability Zones



- Auto scaling for automated instance recovery and scaling
- Using the Amazon Relational Database Service (RDS) with automated backup, recovery and operational monitoring
- Elastic IP Addresses that can be mapped between instances
- Using Amazon S3 simple, durable, massively scalable data storage

The complete infrastructure is built from code and deployed through automated pipelines, from the Virtual Private Cloud (VPC) network layer up to the web application instances.

Data and assets are versioned, backed up and monitored.

17. Incident Management

ReadyTech has documented Incident Response, Business Continuity, Disaster Recovery, Security and Data Breach Response, and Crisis Management Plans that are tested at least annually.

Customers will be notified in accordance with our Incident response or Data Breach response plans in the case of an incident, the timing of which is outlined in the relevant plans and is based on the severity and urgency. The nominated role at ReadyTech will continue to communicate with the customer on the specified schedule at a minimum until the issue is resolved. In general, ReadyTech takes the approach of informing the customer as soon as is practical in all cases.

18. Third Party Supplier Management

ReadyTech relies on sub-service organisations, such as AWS, to run its business efficiently. We evaluate and qualify our vendors with a risk-based approach and documented standards which include security, technical and financial assessments. ReadyTech ensures our security posture is maintained through legal agreements and regular security compliance review of these arrangements.



19. Contacts

ReadyTech is continually striving to keep our systems secure. If you become aware of any security issue or have any further queries regarding this document, please contact the security team directly at security@readytech.io.

20. Classification

This document is **Public**; it is approved for public release.

21. Document Management

Version	Date	Initials	Description
1.0	01/07/2021	SG	Prepared for distribution
1.1	22/02/2023	SG	Minor updates, link fixes
1.2	16/10/2025	EX	Review
1.3	18/06/2026	MT	Penetration Testing methodology update, General review