readytech

VETtrak
Security Processes

August 2023

Table of Contents

1. Introduction

VETtrak is an application suite used by Training Services Providers to manage their operations. Making sure your data is secure and protecting it is one of ReadyTech's most important responsibilities. We are committed to being transparent about our security practices and helping you understand our approach. This document has been written primarily around the security and operations of our hosted services.

2. Services provided

VETtrak software provides many functions and features to our end users. These are documented in detail on our website at VETtrak Features however, a summary has been provided below of some of the major functionality.

2.1.1 VETtrak Software

The core desktop application used by the training organisation administrator to manage records relating to the student and learning environment including reporting and generation of AVETMISS files.

2.1.2 VETtrak Web Portal Products

VEttrak has several web-based portals that are designed for trainers and students to manage their information within the platform, including but not limited to: Trainer Portal, Student Portal, VETenrol, VETsurvey, Progress Portal, VETembark.

VETenrol, A web-based portal for students to view and self-enrol into various training courses offered by the training provider is available amongst other functionality in other portals.

2.1.3 API (Application Programming Interface) connector

The VETtrak API is an open API that allows integrations with other services. This can be used for a multitude of tasks from bulk enrolling students to creating an interactive website for the end user. https://www.vettrak.com.au/software/apis/technical-documentation/

3. 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 27001:2013 certificate is available on the JAS-ANZ register: https://register.jas-anz.org/certified-organisations (search "ReadyTech - Education & Work Pathways")

3.1 Data Sovereignty

VETtrak hosting uses a combination of VETtrak's private cloud and the AWS (Amazon Web Services) Sydney region to ensure data is stored and processed within Australia. Software delivered by VETtrak's

private cloud is also hosted in Australia on ReadyTech owned and operated hardware managed by inhouse staff. ReadyTech will notify customers if any changes in data sovereignty are planned.

For locally installed customers, data sovereignty is the responsibility of the customer.

3.2 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

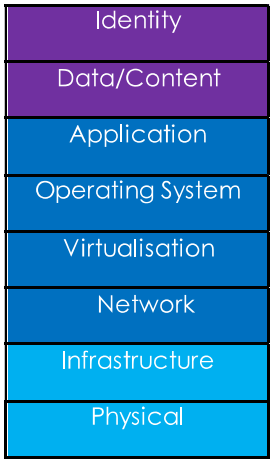
4. Shared Security Responsibility Model

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

4.1 VETtrak Hosted Service

While we manage security *of* the application, security *in* the application is the responsibility of the customer. VETtrak is provided as software-as-a-service, i.e., a fully functioning modern application delivered over the internet. ReadyTech is responsible for procuring, configuring, monitoring, and maintaining all aspects of the computing environment, from the servers to the application.

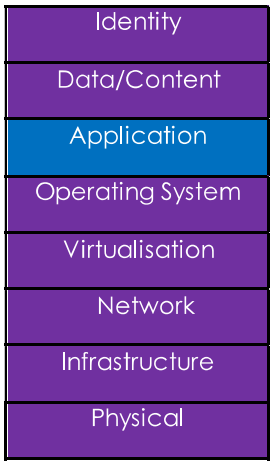
The customer is responsible for managing the access of their authorised users, password policies and configuring roles and permissions within the application itself.



	Customer Responsibility	Security **in** the application
	ReadyTech Responsibility	Security **of** the application
	AWS Public Cloud and ReadyTech Private Cloud Shared Responsibility	Security **of** the cloud

4.2 VETtrak Local Install

While ReadyTech manage security *of* the application, all other aspects of the security ecosystem are the responsibility of the customer. This ranges from the physical security of servers up to the identity management of the users. ReadyTech however still manages the security at the application layer to ensure a safety, security, and integrity of the software applications.



	Customer Responsibility	Security **in** the application
	ReadyTech Responsibility	Security **of** the application

5. 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 Chief Information Security Officer who is responsible for the performance of the ISMS. All staff have security responsibilities assigned as part of their roles.

6. Identity and Access Management

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

- Multi-Factor Authentication
- Role-Based Access Control (RBAC) for configurable, granular provision of permissions and functionality to users.
- Configurable password length and complexity requirements

We recommend the usage of SSO for web portals, however if not used all user passwords are salted and hashed using PBKDF2 to generate 512-bit password hashes using HMAC-SHA512, with 10,000 iterations and 256-bit cryptographically random salts.

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. 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. Access reviews for privileged users are conducted quarterly.

7. Standard Operating Environments

For the ReadyTech hosted environment we use a documented Standard Operating Environment for all servers. The servers are provisioned through code where possible and all change to the environment goes through ReadyTech secure programming practices.

For locally installed customers, operating environments is the responsibility of the customer.

8. Patch Management

Operating systems automatically apply security updates as required. 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.

For locally installed customers, patch management is the responsibility of the customer.

9. 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, QA and UAT.

Access to code repositories is strictly limited.

10. 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 and application frameworks minimizing 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.

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

For locally installed customers, database security is the responsibility of the customer.

11. Network Security

For the hosted service, ReadyTech divides its systems into separate networks (VLANs (Virtual Local Area Network)) to better protect more sensitive data. Systems supporting testing and development activities are hosted on a separate network from production systems.

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

The VETtrak system uses a shared everything multitenancy model. Each application instance hosts the operations of multiple tenants. Logical separation of tenants is controlled by application and operating system security.

VETtrak uses Web Application Firewalls (WAF) that helps protect web applications and APIs (Application Programming Interfaces) against common web exploits. Configured rulesets also provide geo-filtering of traffic from high-risk countries outside Australia. Traffic is also inspected for unwanted content and Anti-virus software is installed on all endpoints.

The desktop application is delivered by Remote Desktop Protocol over TLS via RDP (Remote Desktop Protocol) Remote Gateway. This ensures the confidentiality and integrity of the services being delivered. All web products hosted by ReadyTech are delivered using TLS on port 443.

For locally installed customers, network security is the responsibility of the customer.

12. Cryptography

Data in transit, is only encrypted with ASD (Australian Signals Directorate) Approved Cryptographic Algorithms (AACAs) and ASD Approved Cryptographic Protocols (AACPs).

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 1.2 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. TLS 1.3 will be enabled once supported by our systems.

AWS S3 is used for storage of documents. 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 (60 minutes) URLs. S3 offers 99.999999999% durability by storing the

object on multiple devices within multiple zones within the AWS Sydney region. See https://aws.amazon.com/s3/faqs/ for further information on the S3 service.

For locally installed customers, cryptography selection and usage are the responsibility of the customer.

13. Logging and Monitoring

Site uptime, host and application performance is monitored by internal systems with operational alerting and response procedures in place. Regular governance meetings and performance review ensure the ongoing performance and availability targets are met and that suitable resources exist to scale up the service as required

ReadyTech use Host Intrusion Detection, Network Intrusion Detection Management systems. Alerts are centrally monitored and acted upon by responsible teams. Automatic clock synchronisation with NTP (Network Time Protocol) servers is enabled on all servers.

For locally installed customers, logging and monitoring of the environment is the responsibility of the customer.

14. Backup Management

The system uses multiple backup systems including SQL Clustering, SQL log shipping, secondary and tertiary offsite SQL servers to maintain a redundant and consistent standby copy of the data in separate locations. Database integrity is managed via Microsoft SQL server.

Multiple systems monitor the health of the database instances and initiates a failover automatically in response to a variety of failure conditions.

Note that backups are engineered around disaster recovery. Any requirement to roll back from user error can be managed within the application or with the data services team.

For locally installed customers, backup management is the responsibility of the customer.

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. Note that backups are immutable and will automatically expire as required by lifecycle rules. Data will be made available in standard, documented formats. This will be a Microsoft SQL Server database backup, XLS or TXT exports can also be generated by the user, however other formats may incur a cost.

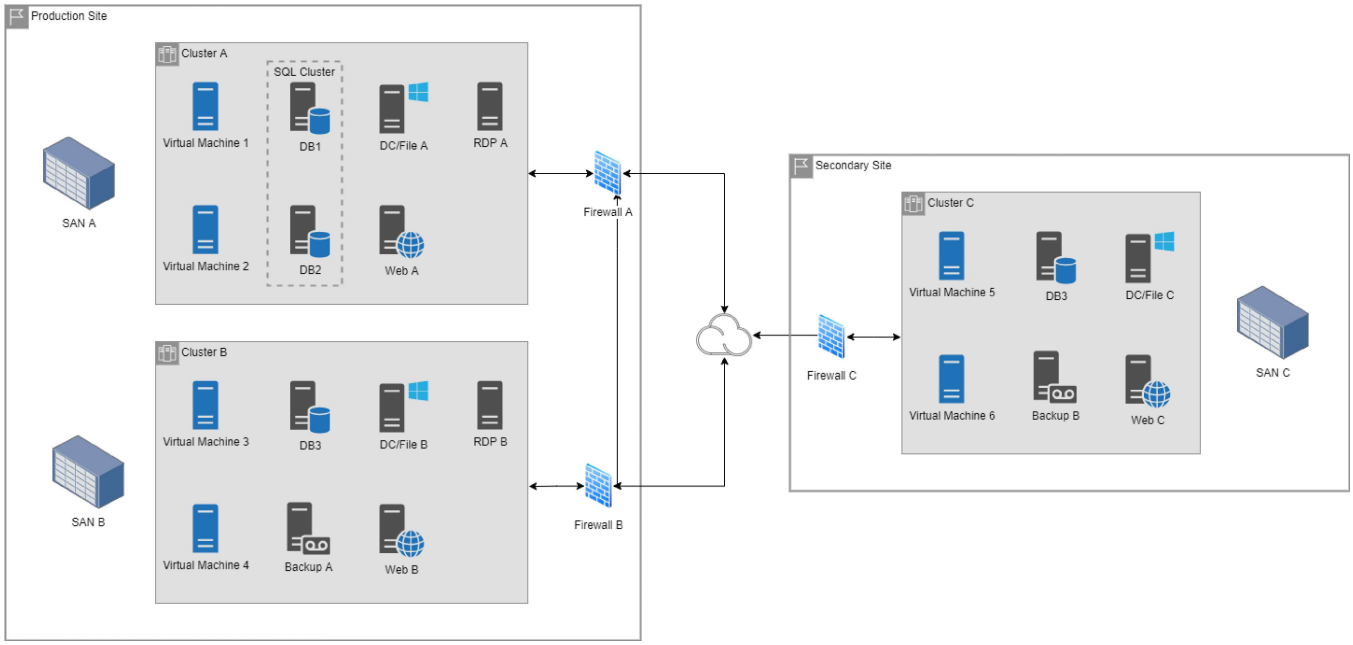
Full database backups are performed nightly and retained for a minimum of 30 days and deleted by automated lifecycle policies.

Processes to destroy data will depend on the location and format of the data, however crypto shredding, removal of the data or processes from NIST Special Publication 800-88 Guidelines for Media Sanitization would be used to ensure complete sanatisation.

For locally installed customers, data retention is the responsibility of the customer.

16. Business Continuity

The concepts of business continuity and disaster recovery are integrated into our design and architecture of our highly available systems in the public cloud. Failure is routinely expected, planned for, tested, and managed with a mix of automated and manual systems and redundancy. An example of the N+1 architecture can be found below.



Uptime and service status of the hosted system can be found at http://vettrak.statuspage.io Document storage is addressed on AWS through using Amazon S3's durable and massively scalable data storage.

For locally installed customers, business continuity is the responsibility of the customer.

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.

If you have an incident or need to contact us, please reference the Contacts section later in this document.

For locally installed customers, incident management is the responsibility of the customer.

18. Third Party Supplier Management

ReadyTech relies on sub-service organisations, such as AWS and our co-location vendor 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.

For locally installed customers, supplier management is the responsibility of the customer.

19. Data Destruction

The process to destroy data or media depends on the location and format of the infomation to be destroyed, however crypto shredding, deletion, or removal of the data or if required processes from NIST Special Publication 800-88 Guidelines for Media Sanitization would be used to ensure complete sanatisation.

20. 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.

If you believe you have found a security vulnerability, please see our Vulnerability Disclosure Policy

https://www.readytech.com.au/vulnerability-disclosure

21. Classification

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

22. Document Management

Version	Date	Initials	Description
1.0	23/05/2022	MN	Prepared for distribution
1.01	26/05/2022	MN/BD/SG	Review
1.0.2	07/08/2023	PB	Minor format changes and removal of SAML 2.0 references