readytech

Ready Community Security Processes

June 2024

Table of Contents

1. Introduction

Ready Community (formerly known as "Open Office") provides an end-to-end solution for local government encompassing Financials, Property and Rating, Asset Management, Licensing, Compliance and Local Services.

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.

3. Shared Security Responsibility Model

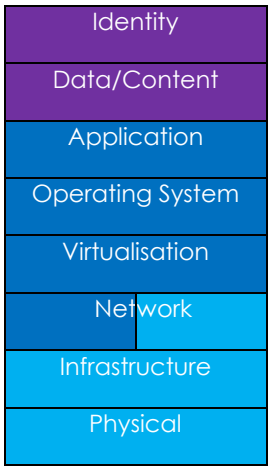
ReadyTech strives to protect the confidentiality, integrity and availability of all critical information and stored customer data.

While we manage security of the application, security in the application is the responsibility of the customer.

ReadyTech is responsible for procuring, configuring, monitoring and maintaining all aspects of the computing environment, from the servers to the application. ReadyTech utilises Microsoft Azure, which is a world leading provider of cloud infrastructure.

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

In the Azure Hosted Environment:



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

3.1 Infrastructure

Our system is hosted in the public cloud with Microsoft Azure. Microsoft Azure provides state-of-the-art data centres and a world-leading compliance program. Microsoft Azure operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which our system operates. Microsoft Azure manages the network devices, but ReadyTech is responsible for secure network configuration.

3.2 Data Sovereignty

We use Microsoft Azure data centres close to our clients, in Australia, to ensure best performance and so that data is stored and processed within local data sovereignty.

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 Chief Information Security Officer 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

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

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

When the system is configured to use the native password authentication, password length and complexity requirements are enforced by the system. Password expiration can be configured or disabled entirely.

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.

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 parameterized. 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 minimizing any exposure through direct database access.

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 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 minimize the potential attack surface for malicious actors. Changes to the production network configuration are restricted to authorised personnel and all changes logged.

11. Cryptography

Data at rest, and in transit, is only encrypted with ASD 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.

Azure Blob is used for storage of documents and other unstructured data. Blobs are securely configured, objects are private and encrypted at rest using AES-256.

Structured data stored in SQL Server is encrypted at rest using AES-256.

12. Logging and Monitoring

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

13. Penetration Testing

ReadyTech build applications using the Open Web Application Security Project (OWASP) Standard. (www.owasp.org) This standard provides a framework for developers, implementers and infrastructure deployments to build secure applications.

When software applications are penetrated tested the OWASP standard is used to ensure that best practice security is in place. Penetration tests examine the application and the underlying infrastructure response to an attack. ReadyTech integrate the OWSAP Standard into all stages of the software lifecycle. The standard is constantly reviewed and updated to ensure any new threats are incorporated.

As applications are deployed into single tenancies, customers may engage independent, CREST certified entities to conduct application penetration tests at any time.

Results of these tests are shared with ReadyTech management and available to customers under NDA. Findings are reviewed, prioritised and tracked to resolution.

14. Backup Management

ReadyTech perform database backups every night and for Azure SQL implementations every 5 minutes. ReadyTech provide a 30 day restore point as a default backup service. Backups are retained for 30 days.

Monthly Database Backups are performed on the last day of each month and retailed for 12 months.

Yearly Database Backups are performed in week 26 of each year and retained for 2 years.

Monthly and Yearly backups can be transferred into a customer's local environment using a backup agent or as requested.

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 via the platform.

Database backups are retained for 90 days and deleted by automated lifecycle policies.

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 in the cloud through:

- Running full recovery mode on databases to allow for point in time restoration

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 Microsoft Azure, 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	1/07/2022	CM/SG	Prepared for distribution
1.1	13/07/2023	DR	Adjusted the 14. Backup statement
1.2	19/06/2024	AK	Renamed the document and have removed the single tenancy items from network security