readytech

CouncilWise Security Processes

September 2025

Table of Contents

1. Introduction

CouncilWise is a comprehensive local government management platform that streamlines and connects critical functions across the community, including property and rating, land management, infringements, receipting, licences and permits, and more. providing councils with a unified system designed to enhance efficiency, accuracy, and service delivery.

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. All ReadyTech segments are certified using the ISO 27000 standards and we are working towards Councilwise completion of ISO 27001 certification.

3. Shared Security Responsibility Model

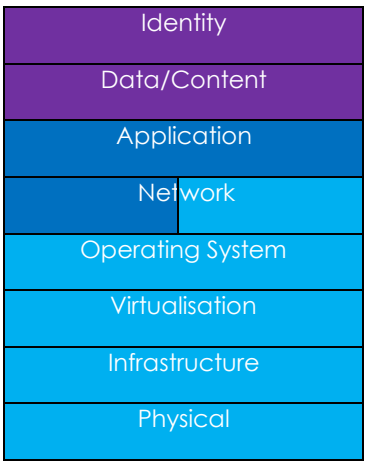
ReadyTech strives to protect the confidentiality, integrity and availability of all critical information and stored customer data.

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. CouncilWise utilises Microsoft Azure, which is a world leading provider of cloud infrastructure.

Our customers are responsible for managing the access of their authorised users, and configuring access policies 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 virtualisation 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

Secure access control for the CouncilWise platform is provided through the Microsoft identity platform within each customer's Azure AD tenancy. This ensures customers retain full control over authentication, including Multi-Factor Authentication, authorisation policies, and Role-Based Access Control for application features, leveraging services within the customers tenancy, such as SharePoint for document management.

In-application Councilwise implements a Fine-Grained Module based permission system for granular provision of permissions and functionality to users.

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

Standard Operating Environment for the CouncilWise platform is defined and documented for all Azure App Service environments. Provisioning is managed through Infrastructure as Code, and every change adheres to CouncilWise's secure development and deployment practices.

7. Patch Management

Security updates and patch management are handled by Azure platform services.
Application vulnerabilities are identified through automated monitoring systems.
The patching of application components is incorporated into regular software development procedures and release schedules.
Critical issues and security patches may require an out-of-cycle release, which is processed through the standard change management workflow.

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, UAT 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.

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

Network access to all environments 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.

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.

SharePoint within the customer's tenancy is used for storage of documents and other unstructured data. Documents remain under the customer's direct control within their own environment, with built-in benefits including version history, audit trails, and compliance with their existing security policies. SharePoint provides enterprise-grade encryption at rest and in transit, ensuring document security while maintaining customer data sovereignty.

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 penetration 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.

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

Customer databases leverage Azure SQL backup and retention service. Transaction log backups are taken every 5-10 minutes allowing Databases to be restored to any point in time in the last 28 days.

Differential backups are taken every 12 hours and full backups are taken once per week (the exact day/time full backups occur is determined by the service and is not configurable.

Weekly Database backups are retained for 1 year

Monthly Database backups are retained for 3 years (The first full backup of the month)

Yearly Database backups are retained for 10 years (26th week of the year)

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
- Versioning, backup and monitoring of all data and assets
- Scalable application and database platform services that enable rapid scaling and provisioning
- Distributed, independent application environments that isolate failures to a subset of customers and enable rapid rerouting to unaffected environments

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	1/10/2025	BW	Prepared for distribution