ReadyTech Shared Responsibility Model

V21.1

Document Control

Version	Date	Initials	Description
1.0	1/12/2020	SG	Prepared for distribution
1.0.1	18/01/2021	SG	Review
1.0.2	09/07/2021	SG	Internal review

Table of Contents

1 Shared Responsibility Model

Security and compliance are shared responsibilities between ReadyTech and the customer. This shared model helps relieve customers from the operational burden of developing and managing IT applications, which enables them to reallocate security resources and budget to other business priorities.

ReadyTech protects the confidentiality, integrity and availability of all critical information and customer data that is processed by its software during transfer, processing, and storage using industry-standard measures.

The customer is responsible for ensuring the software meets their security, regulatory and compliance requirements, including managing the access of their authorised users and configuring roles, permissions and system functionality within the software itself. The customer is responsible for their user devices, networks and the communication layers that connect their users to the software.

ReadyTech collects and processes data on behalf of the customer in accordance with the Privacy Policy. The security and privacy measures implemented by ReadyTech are detailed in the Privacy Policy: https://www.readytech.io/privacy

Details of how we process personal data processed by our platforms, are set out in the Data Processing Addendum:
https://www.readytech.io/legal/dpa

2 Software as a Service

Within our software-as-a-service offerings, ReadyTech is responsible for procuring, configuring, monitoring, and maintaining all aspects of the computing environment, from the servers to the application. ReadyTech utilises either third party Infrastructure as a Service (IaaS) suppliers, like Amazon Web Services (AWS) and Microsoft Azure, or colocation within third party data centres. ReadyTech manages the secure configuration, use and regular review of vendors to ensure that services meet our security standards.

2.1 Service Provider Security Responsibilities

Our IaaS and colocation service providers have responsibility for the following items:

- Physical security of the infrastructure, including but not limited to, equipment selection; power supply assurance; cooling facilities; protection against fire, water, shock, and theft; and surveillance
- Security of compute, storage, database and network software
- Security of networks, such as firewalls and distributed denial of service (DDOS) protection
- Security of cloud storage, including encryption, backup and recovery
- Security of infrastructure virtualisation, such as tenant resource isolation and virtualisation resource management

- Security of the application software, operating system, database and supporting services
- Tenant identity management and provisioning of initial access
- Secure access to cloud resources by tenant
- Security management, testing, operations, monitoring, and emergency response
- Service continuity assurance and disaster recovery plans

2.2 Cloud Customers' Security Responsibilities

Our customers are responsible for the following:

- User identity management and access control within the software
- Data security, and ensuring the relevant platform meets all relevant regulatory and compliance requirements
- Security management of devices that access cloud services, including hardware, software, application systems, and device rights

3 Self-hosted

Within our self-hosted offerings, ReadyTech provides software that is secured using industry-standard measures. The customer takes on the responsibility of configuring the software to meet their requirements and secure delivery of all the IT services necessary to operate the software and update as required from time to time.

4 Contacts

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.