JR Live: Overview of Security Processes

November 2020

Document Control

Version	Date	Initials	Description
1.0	24/11/2020	AB / SG	Prepared for distribution

Table of Contents

1 Introduction

JR Live is an enterprise web application used by Employment 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.

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 27001:2013 certificate is available on the JAS-ANZ register:
https://www.jas-anz.org/our-directory/certified-organisations/5b8e9707-b16c-4914-9750-be240d6a6b16

The cloud hosting platform is designed to meet the requirements and security controls of the Australian Government's *Information Security Manual (ISM)* and Australian Signals Directorate (ASD) cloud security guidance for storage and processing of data classified up to *Unclassified DLM (Dissemination Limiting Marker).*

JR Live has been accredited by the Department of Education, Skills and Employment as meeting the standards required by the Third Party Employment System Accreditation Program after a rigorous audit process. The Department have issued an Accreditation letter which can be found on their site and outlines the responsibilities that an Employment Service Provider must implement to use JobReady Live securely.
https://www.employment.gov.au/digital-information-assurance

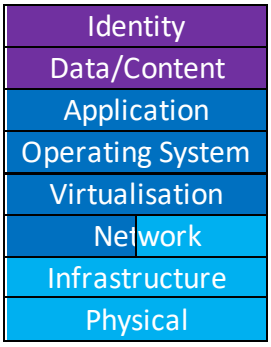
3 Shared Security Responsibility Model

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. JR Live 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://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

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

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: https://www.readytech.com.au/privacy



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

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

JR Live 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.

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 client 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

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

- a SAML 2.0 compliant Service Provider interface
- Role-Based Access Control (RBAC) for configurable, granular provision of permissions and functionality to users.

We recommend the usage of SSO. If the internal username/password capability is used, passphrases have length and complexity requirements to IRAP standards, and are salted and hashed at rest using bcrypt.

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 (multifactor authentication). 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 (User Acceptance Testing).

Access to release branches in the code version repository is 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 (Open Web Application Security Project) security guidelines. Database queries are parameterized. Application inputs and outputs are properly sanitised and encoded. Errors and exceptions are logged and monitored.

9 Database Systems

Each client uses a logically isolated database schema. All use and administration of the database is through the web 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. All database data is encrypted at rest using AES-256 with secure key management procedures.

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

10 Network Security

ReadyTech divides its systems into separate networks (AWS VPCs (Virtual Private Cloud)) 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. A dedicated AWS Account is used for the JobReady Live system, separate from all other ReadyTech products and services.

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. ReadyTech uses an Infrastructure as Code approach to the network configuration which uses versioned repositories and is deployed through automations to avoid potential misconfiguration.

The JobReady Live system uses a shared everything multitenancy model. Each application instance hosts the operations of multiple tenants in its own internal address and control space. Logical separation of tenants is controlled by application logic at runtime. Each tenant uses an isolated DNS subdomain to access the application and has a logically isolated database schema.

All public facing internet connections leverage an AWS Application Load Balancer and AWS Shield for a managed Distributed Denial of Service (DDoS) protection service.

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards web applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency. AWS Shield defends against most common, frequently occurring network and transport layer DDoS attacks without any input from JobReady.

Live uses AWS WAF, a web application firewall that helps protect web applications or APIs against common web exploits. Configured rulesets also provide geo-filtering of traffic from outside Australia to meet ISM requirements.

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.

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 (60 minutes) URLs.

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.

ReadyTech use Host Intrusion Detection, Network Intrusion Detection and Cloud Security Posture 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.

13 Penetration Testing

ReadyTech engages independent, CREST certified entities to conduct application penetration tests annually. Results of these tests are shared with ReadyTech management and available to customers under NDA. Findings are reviewed, prioritised, and tracked to resolution. Customers wishing to conduct their own penetration test of the JR Live application should obtain permission from ReadyTech.

14 Backup Management

Live uses a Multi-AZ configuration of the Amazon RDS (Relational Database Service) to maintain a redundant and consistent standby copy of the data in different Availability Zones (AZs). Multi-AZ deployments of the PostgreSQL engine utilize synchronous physical replication to keep data on the standby up to date with the primary.

Amazon RDS monitors the health of the database instances and initiates a failover automatically in response to a variety of failure conditions including loss of availability in an Availability Zone, loss of network connectivity to the instance, and compute failure or storage failure. DB instance failover is fully automatic and requires no administrative intervention. Availability impact is limited to the time automatic fail-over takes to complete which is typically one to two minutes.

Recovery Point Objective (RPO): < 1 minute.
Recovery Time Objective (RTO): 2 minutes.

Complete logical backups of the database are stored in S3 daily, offering 99.999999999% durability. An independent automated process validates that backups are present and

accounted for daily. Production data backups are regularly restored to the staging server for validation and to use current data for staging QA purposes.

15 Data Retention

Data is retained within the system for the life of the contract. At contract termination, data is returned and removed according to standard operating procedures.
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 Multi-AZ Amazon Relational Database Service (RDS) for multiple Availability Zone managed databases
- 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.

Clients 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 your data 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.