readytech

Ready Workforce Talent Security Processes

March 2025

Table of Contents

1. Introduction

Ready Workforce Talent is a cloud-based talent management system designed to optimize employee performance and drive organizational success. As a comprehensive solution, it integrates seamlessly with existing HR infrastructure, providing a powerful platform for workforce development. Talent offers a modular and highly customizable system, allowing businesses to nurture their most valuable asset – their people.

Talent was founded with a vision to transform organizations through innovative talent management solutions.

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. Services Provided

Ready Workforce Talent software offers a wide range of functions and features for end users. Below is a summary of some the major functionalities:

360 Feedback: Anonymous peer feedback, with self-rating and manager reviews to create holistic view of top strengths and improvement.
Competency Management: Review skills or behavioral traits to help Identify and address competency gaps.
9 Box Grid Talent Management: Talent mapping to view team performance and potential across departments.
Compliance Training: Ensure organization meets legal and regulatory requirements, minimizing risk and promoting accountability.
Course Builder: Easily design custom training programs to meet specific needs with an intuitive course builder tool.
Learning Management: Deliver targeted training and development opportunities, facilitating continuous learning and career growth.

License & Certification Tracking: Streamline the management of professional credentials, ensuring compliance and up-to-date certification for your workforce.

Onboarding & Inductions: Streamline the integration of new employees, ensuring a smooth and welcoming introduction to your company culture and values.

Performance Management: Track individual or team performance, goals, and development plans.

Skills Management: Track and develop employee skills.

Succession Planning: Prepare for future leadership by measuring competency and talent strength between employees.

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

ReadyTech are annually reviewed by the ATO to meet the DSP Operational Security framework.

4. Shared Security Responsibility Model

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

4.1 ReadyTech's Role

ReadyTech is responsible for the security of the software. ReadyTech is responsible for the overall delivery, maintenance, and support of the service. This includes managing the application, ensuring data security, and providing client support.

4.2 Client's Role

While we, as the SaaS provider, are committed to implementing robust security measures to protect the client data, it's essential that the client also play an active role in securing the content. The client's actions are critical in maintaining the overall security of the system and safeguarding the information.

1. Access Control Management:
   - Ensure that only authorized personnel have access to the system by regularly reviewing the user and administrator permissions.
   - Implement strong password policies to prevent unauthorized access.
2. Data Handling Practices:
   - Exercise caution when uploading, downloading, or sharing data to avoid accidental exposure.
3. Incident Reporting:
   - Promptly report any suspicious activities or potential security incidents to ReadyTech so that we can take immediate action to mitigate risks.
   - Collaborate with ReadyTech during security investigations to ensure quick and effective resolutions.
4. Compliance with Security Policies:
   - Ensure that internal practices align with industry standards and any regulatory requirements specific to the organization.

In summary, the client manages the security ***in*** the software. This means ReadyTech does not handle issues such as password complexity but provides the tools for clients to enforce these policies if desired.

The Talent application supports configuration of:

- Password policies
- MFA
- SAML 2.0 SSO Service Provider interface
- Role-Based Access Control

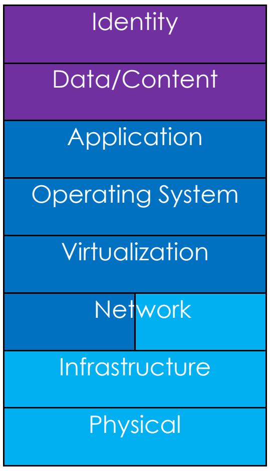
ReadyTech utilises Amazon Web Services (AWS), which is the world leading provider of cloud infrastructure. AWS physical and technical security practices are outlined in its whitepaper at https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

Examples include:

ReadyTech: Takes care of physical security, platform security, data security, and application security, including secure development, bug fixing, and software application patching.

Customer: Manages password resets, complexity, MFA requirements, access roles, and all aspects of security within the software.

AWS: Manages the security of the cloud, including the physical security of data centers, network infrastructure, and foundational cloud services. AWS is responsible for securing the underlying hardware, and global network that support the cloud environment. This includes redundancy, compliance certifications, and operational security to protect against threats at the infrastructure level.



Identity

Data/Content

Application

Operating System

Virtualization

Network

Infrastructure

Physical

🟪	Customer Responsibility	Security **in** the application
🟦	ReadyTech Responsibility	Security **of** the application
🔷	AWS Responsibility	Security **of** the cloud

4.3 Infrastructure

Ready Workforce Talent is hosted in the public cloud with AWS. AWS provides state-of-the-art data centers 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 Ready Workforce Talent operates. AWS manages the network devices, but ReadyTech is responsible for secure network configuration.

4.4 Data Sovereignty

Ready Workforce Talent only uses the AWS Sydney region to ensure data is stored and processed within Australia. Data is not transferred out of Australia.

4.5 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

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

Ready Workforce Talent provides out of the box functionality to support secure access control for customers:

- **Single Sign-On (SSO).** Any SSO via SAML 2.0 is supported. Okta, Azure AD (Entra), and other common identity providers are also supported via SAML 2.0.

- **MFA (Multi-Factor Authentication)** for password-authenticated users.

- **Role-Based Access Control (RBAC)** for configurable, granular provision of permissions and functionality to users. This can be set up with **"*security groups*"**. A Security Group defines a common set of permissions that you can apply to selected administrators such as if you have groups of administrators who all require the same set of permissions, for example, Regional Administrators Security Group. An unlimited number of Security Groups can be created.

- **Other Authentication Hardening Options.** When the system is configured to use the native password authentication, administrators can configure additional authentication policies from the global security settings to enhance account security. Below are key configurable options:

    - **Password Policies**
        - **Password Length:** Defines the minimum number of characters
        - **Password Complexity:** Ensures passwords contain the specified character criteria
        - **Password Expiry:** Passwords can also be set to expire after a defined period
        - **Password History**: Controls how many previous passwords an admin or employee must avoid reusing
        - **Password Reset Token Expiry**: Determines how long a password reset link remains valid
    - **Login Behavior and Time-Saving Options**
        - **Session Expiry:** Defines how long a user can stay logged in before they must log in again
    - **Account Lockout and Security Measures**
        - **Failed Login Attempt Lockout:** Locks an account after a specified number of failed login attempts
        - **Lockout Duration:** Specifies how long an account remains locked after reaching the failed login attempt limit

These measures help enforce strong authentication practices and prevent unauthorized access.

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. 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.

7. Standard Operating Environments

Ready Workforce Talent utilizes a **documented Standard Operating Environment (SOE)** for all servers to ensure consistency, security, and maintainability. Servers are configured according to **industry best practices**, with standardized operating system versions, security settings, and software dependencies.

All changes to the environment go through **Talent's change management process**, which includes **testing, approval workflows, and controlled deployments** to minimize risks and maintain system stability. Regular updates and security patches are applied as part of our ongoing maintenance strategy.

8. Patch Management

Operating systems automatically apply security updates monthly. Application vulnerabilities are identified through automated systems, code review, and testing. 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.

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, 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 and encrypted.

10. Database Systems

When hosting through Ready Workforce Talent's AWS environment, 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.

11. Network Security

ReadyTech divides its systems into separate networks (AWS VPCs) 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 network.

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 authorized personnel and all changes logged.

12. 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 1.3 with Elliptic Curve Diffie-Helman session keys and perfect forward secrecy. SSLv3, TLSv1.0 and TLSv1.1 are disabled. A TLS connection is enforced.

All client data is stored on Amazon Web Services and never moved off AWS. Production data is stored in EC2 and S3. All client data is stored on encrypted cloud volumes via EBS. All media containing client data are encrypted with at least 256-bit encryption, and all are automatically server-side encrypted using 256-bit Advanced Encryption Standard (AES-256) with keys maintained by AWS.

In addition, we also enforce row-level encryption wherein data encryption is applied to sensitive personal information, including TFN, bank details, superannuation details, and employment contracts. Encrypted data is stored in the application database. The method of encryption is AES-256 in accordance with standards set by the ASD (Australian Signals Directorate) / NIST (National Institute of Standards and Technology), with encryption keys being securely managed per-application.

13. Logging and Monitoring

The application logs login attempts. In addition to that, we use a number of different logs:

- In the application audit log
    - These log changes to user-entered data in performance and development folders
    - Access is controlled by administrators
- In the application email log
    - These log emails sent by and to users
    - Access is controlled by administrators
- Application server logs
    - These log application events, including user log-ins, failed access attempts to system functions
    - They are accessible only by permitted Talent system administration personnel
- Application page requests
    - These log page requests by users through the software
    - They are accessible only by permitted Talent system administration personnel
- Server access logs
    - These log login activity by each Talent system administrator
    - They are accessible only by permitted Talent system administration personnel
- Server file auditing
    - This logs changes to files and can be tracked in individual Talent system administrator accounts
    - They are accessible only by permitted Talent system administration personnel
- IDS and IPS logs
    - These log the triggering of IDS and IPS rules. These are security-related system alerts and failures
    - They are accessible only by permitted Talent system administration personnel
- Other
    - Outbound emails sent by the application
    - Application errors
    - Backup success/failure

We preserve user event logs in case of a breach or need for investigation.

We utilize an IDS and IPS with real-time logging and alerting. IDS detects, blocks, and logs unauthorized access attempts to the network and system. OS-level security also logs all login attempts. Application-level security also logs all access attempts. OS-level events are retained for a period of 1 month. Application-level logs are retained for the archival period of 7 years. IDS/IPS retains security events for 32 days and system events for 91 days.

Log information is stored within the application servers and archived on AWS S3.

14. 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 Talent application should obtain permission from ReadyTech.

15. Backup Management

Daily snapshots are taken to ensure a failed volume can be recovered.

Data at rest stored in AWS S3 is automatically server-side encrypted using 256-bit Advanced Encryption Standard (AES-256) with keys maintained by AWS.

Backup media is rotated into Amazon Glacier for archival, and is automatically server-side encrypted using 256-bit Advanced Encryption Standard (AES-256) with keys maintained by AWS.

Backups are performed on a daily basis and are kept in high-availability storage for **14 days**. Weekly archives are kept in cold storage for **7 years** or upon client's contract cessation. Once expired, client data is deleted securely, making it unrecoverable by using industry-standard data sanitization techniques. AWS S3 support Secure Erase functionality, which overwrites the data to prevent recovery.

We implement controls to govern the retention and purging of information within our data management framework. Our approach is designed to ensure both compliance with relevant regulations and the protection of sensitive data throughout its lifecycle.

Key controls include:

Retention Policies: On cessation of the contract term (or upon the client's request to delete data), all client data is deleted. The decommissioning process requires two levels of approvals from our CEO and Customer Success Advisors.

Automated Systems: Upon cessation of a client contract, all client data are purged from our AWS servers and storage media, including backups. The files are deleted in a manner that is compliant with our security policies. Once expired, client data is deleted securely, making it unrecoverable by using industry-standard data sanitization techniques. AWS S3 supports Secure Erase functionality, which overwrites the data to prevent recovery.

Data Classification: Media storage devices used to store client data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life-cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored client data is not removed from AWS control until it has been securely decommissioned.

By implementing these controls, we ensure that information is retained only as long as necessary and is purged securely when it is no longer needed. This approach aligns with our commitment to data privacy, security, and compliance.

16. Data Retention

Client data will be deleted after seven (7) years or on cessation of the contract term.

Backups are retained for up to seven (7) years and deleted by automated lifecycle policies.

Once expired, client data is deleted securely, making it unrecoverable by using industry-standard data sanitization techniques. AWS S3 supports Secure Erase functionality, which overwrites the data to prevent recovery.

Our clients can access their data through exportable reports at any time. This includes during a contract term and just prior to cessation of a contract term. Assistance to extract data can be provided as a separate service if needed.

17. 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 full recovery mode on databases to allow for point in time restoration
- Application layer availability and scalability managed through AWS.
- Elastic IP Addresses that can be mapped between instances
- Using Amazon S3 simple, durable, massively scalable data storage

Data and assets are versioned, backed up and monitored.

18. 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.

19. Third Party Supplier Management

ReadyTech relies on sub-service organizations, 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.

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.

21. Classification

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

22. Document Management

Version	Date	Initials	Description
1.0	03/03/2025	OW, CRD	Prepared for distribution