



RFFR Accreditation for

Ready Recruit by ReadyTech

Ready Recruit is a platform designed to support Group Training Organisations (GTOs) in managing apprenticeship programs. It provides tools to streamline recruitment, placement, and administrative processes, with a focus on improving operational efficiency and apprenticeship completion rates.

Ready Recruit has been accredited by the Department under the RFFR assurance approach as a Third-Party Employment and Skills (TPES) system. ReadyTech has demonstrated an effective Information Security Management System (ISMS), independently certified to ISO/IEC 27001:2022.

While RFFR accreditation provides assurance over the system's security controls, consumer organisations remain responsible for managing security within your own use of the system. Consumers must review the shared responsibility model, along with the security practices and procedures published on ReadyTech's website, to ensure your use of Ready Recruit aligns with RFFR requirements. In addition, the ReadyTech TPES Addendum outlines specific security, incident response, and data handling obligations that apply to all accredited systems and should be reviewed to understand ReadyTech's commitments and your organisation's responsibilities under the agreement.

Key consumer responsibilities include:

- Notifying the Department of your intention to start, expand, or cease use of Ready Recruit
- Conducting your own risk assessments prior to use and demonstrating in your RFFR documentation
- Maintaining the security of your ICT environment and assets used to access Ready Recruit
- Configuring and managing integrations with APIs and external systems, if applicable, including email gateways, messaging services and business intelligence tools
- Configuring system settings through privileged user accounts, including user roles and permissions
- Managing user accounts and access levels (privileged and unprivileged)
- Managing credentials in accordance with your organisation's password/passphrase policy
- Monitoring user access activity and security events
- Enabling and enforcing multi-factor authentication (MFA), configuring Single-Sign-On (SSO)
- Managing the export of data and reports in accordance with your organisation's security policies
- Managing the security of document uploads, scanned records and digital forms

The Department reserves the right to clarify the Accreditation boundaries at any time. The Accreditation does not imply endorsement or guarantee of system security. In the event of a cyber incident involving Ready Recruit, consumer organisations remain responsible for managing your own response, including notification, containment, and remediation activities. The Department may request information to support its oversight responsibilities and assess any broader impacts to government programs.