Australian Government
Department of Employment and Workplace Relations

RFFR Accreditation for

Esher House by ReadyTech

Esher House provides behavioural assessment tools and structured intervention programs to support employment services. The system applies evidence-based methodologies to assess job seeker attitudes and readiness. These assessments enable segmentation and targeted support strategies, helping organisations tailor services that promote sustained employment outcomes.

Esher House 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 Esher House 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 Esher House
- 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 Esher House
- 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
- 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 Esher House, 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.