Australian Government

Department of Education,
Skills and Employment

Your Ref
Our Ref ESES20/814

External Systems Accreditation Authority
First Assistant Secretary – Digital Solutions Division
Kerryn Kovacevic

Accreditation of the third party employment system JobReady Live

This document is to assist employment services providers understand the scope of the accreditation of JobReady Live performed for the Department of Education, Skills and Employment (the department). The accreditation assessment has been performed against the Information Security Manual (ISM) 2017.

Accredited employment programs

JobReady Live has been accredited for use to assist in the delivery of the following employment programs:

- jobactive
- Disability Employment Services (DES)
- ParentsNext
- New Enterprise Incentive Scheme (NEIS)
- Transition to Work (TtW)
- PaTH.

Accredited features and benefits

The following features and benefits of JobReady Live have been accredited for use to assist in the delivery of the above employment programs.

JobReady provides its clients – employment service providers (providers) – with the JobReady Live software-as-a-service to help with workflow management and automation, which includes the following functions:

Feature	Feature description
Employer Customer Relationship Management Module	Gives providers a tool to manage employers/ organisations that the provider is currently working with, as well as prospective employers/ organisations

Feature	Feature description
Vacancy Management Module	Gives providers end to end vacancy management across their organisation using the ESS Vacancy API
Jobseeker Management Module	Management of relationships with their caseload of job seekers
Post-Placement Support Outcome Tracking Module	Manage and track job seekers who are in a placement, ensuring the job seeker is supported whilst also tracking the job seeker through to outcome milestones
Reporting Module	Reports are available covering a broad range of topics such as Performance Management and Outcome/ Claim Management Employer Engagement. File exports are available to users
System Settings (Administration Module)	Gives providers administrative user control over the setup and configuration of their organisation's JobReady Live site including user management, site management, template management, enumeration management and email gateway configuration
Finance Module	Provide finance users with access to manage the Employment Fund Commitment and Reimbursement Process between JobReady Live and ESS using department supported Extensible Mark-up Language (XML) upload/ download process
Jobseeker Portal Module	Self-service access for job seekers to perform actions such as reviewing key documents provided by the provider and view available jobs/ positions
CCU Kanban	An agile management screen that facilitates the management of outcome claims
ESS Integration	Use of the department's ESS system to populate and update JobReady Live with supported data including ES Reporting, Employer API and Vacancy API: o ES Reporting involves downloading subscription data to populate and update JobReady Live o Employer API involves creating employers in ESS based on a record that exists in JobReady Live o Vacancy API involves creating vacancies in ESS based on a record that exists in JobReady Live
Search/ Filtering Data	All modules in JobReady Live provide the user with the ability to filter lists of records to perform ad-hoc reporting, identifying lists of records and performing bulk actions
Document Management	JobReady Live supports the uploading of documents to entity records such as documents scanned from paper or files emailed to consultants

Feature	Feature description
Noting	Notes are used to record comments relating specifically to the entity it is recorded against
Job Match Attributes	Recorded against Jobseeker and Vacancy records, used to allow matching from either entity
Indigenous Mentoring	Manage indigenous mentoring activities such as recording information related to identified barriers, details of intervention provided and time spent
Reverse Marketing	Promote job seekers to prospective employers to produce a position/ opening for them
Jobseeker/ Vacancy Recommendations	Allow providers to put forward a job seeker to a vacancy
Purchase Orders	As part of job seeker management, goods and services may need to be purchased in order to achieve employment and this allows the raising of purchase orders
SMS Communications	Allows SMS to be used to communicate with job seekers and employers. The backend of this service is MessageMedia located in Australia and owned by Message4u Pty Ltd. JobReady provide the integration point with MessageMedia. A provider wishing to use this feature to use MessageMedia to send SMS from JobReady Live will need to hold an account with them, assess and accept the risk of using this feature and product.
Email Communications	Allow outbound emails from JobReady Live to job seekers, employers and provider staff members. Providers can use JobReady's Microsoft Office 365 email gateway or point to their own organisation's gateway.
Document Scanning Module	The document scanning module allows users to generate a Quick Response (QR) Code cover page for a key entity and select the type of document
E-Forms	Allow provider staff to produce their own digital forms for completion within JobReady Live
Dispatchr	Merge information onto Microsoft Word document templates and generate a Portable Document Format (PDF) as output for Purchase Order generation

Feature	Feature description
JobReady Client Hosted Database Access	Provide a facility for providers to connect their Business Intelligence tools to a restored instance of their JobReady Live database
National Crime Check Integration	Perform Australian Police Checks for job seekers using National Crime Check Pty Ltd, which has been accredited by the Australian Crime Intelligence Commission

Excluded features and benefits

There are some features available as add-ons to JobReady Live that have not been covered by the audit at JobReady's discretion, therefore they are not accredited:

- MessageMedia uses job seekers' phone numbers to assist providers with relationship management. JobReady Live provides integration with MessageMedia. Should a provider chose to use this feature, they will need to maintain their own account with MessageMedia. This involves independently assessing MessageMedia as a third party IT provider, and include within their own RFFR accreditation

- PsychPress interactions KnowU, GuideU and DiscoverU functionalities

- JobReady Live provides integration with Esher House CorteX. Should a provider choose to use this feature, they will need to maintain their own account with Esher House CorteX. This involves independently assessing Esher House CorteX as a third party IT provider, and include within their own RFFR accreditation.

Provider responsibilities

To use JobReady Live in an appropriately secure manner, there are actions required on the part of providers.

- Advise the department of your intention to start, expand or cease using JobReady Live.

- All interactions between JobReady Live and the provider's ICT environment are subject to the provider's own assessment under the Right Fit For Risk assurance approach. This includes the use of any excluded features and benefits listed above. Each provider will need to work directly with JobReady to obtain the level of assurance required as part of your assessment of your own environment for these excluded features and benefits.

- JobReady uses an extension of the shared responsibility model to deliver JobReady Live. Amazon Web Services (AWS) is responsible for security **of** the cloud; JobReady is responsible for security **in** the cloud as well as security **of** the application; the provider is responsible for security **in** the application. This means that it is the provider's responsibility to configure JobReady Live appropriately to meet their security requirements. JobReady have confirmed to the department that they have obtained the Certification Letter and Certification Report issued by the ACSC in relation to AWS, and that they have appropriately addressed the items noted within these documents. JobReady will conduct regular security awareness training to providers to promote best practice security and configuration of JobReady Live.

- User access for provider staff is controlled by provider staff. Providers need to determine what roles are required to allow their staff to perform their jobs while maintaining minimum privileges. Providers are also responsible for the timely removal of JobReady Live access when their staff no longer require it.

- Forgotten passwords can be securely reset by each user over email. It is the provider's responsibility to positively identify users during enrolment or manual password resets.

- When using the jobseeker portal there is a risk of a privacy breach if a provider staff member gives access to the wrong job seeker, or if documents (eg a resume) were attached to the wrong portal record. There are no system controls available to prevent such a breach.

- When using MessageMedia, provider staff need to manually validate the job seeker's phone number and the text to be sent to the job seeker, the mobile number is populated initially by JobReady Live. There is a risk of a privacy breach if a provider staff member enters the wrong job seeker's phone number. There are no system controls available to prevent such a breach.

- Web application events such as search histories and viewing customer records are logged but do not form part of JobReady's event logging and monitoring strategy. The provider is responsible to perform these security event log audits covering both the provider's own staff and JobReady staff activity within JobReady Live relating to their job seekers.

- Data imported (exported) to JobReady Live is not immediately scanned for malicious and active content. JobReady Live will accept the importation of files in txt, pdf, doc, docx, xlsx, xls, jpg, jpeg and png file types. Attachments are uploaded into an S3 bucket for document storage, where there is no execution. Where a file cannot be scanned by JobReady Live, the user is presented with a warning that the file has not been scanned. There is reliance on the use of appropriate anti-virus scans and log reviews by the provider and their job seekers using JobReady Live when these documents are downloaded and accessed in their own environments. Providers should perform these monthly audits covering both the provider's own staff and JobReady staff importing (exporting) content to JobReady Live relating to their job seekers.

- When information is introduced onto a system not accredited to handle the information, personnel must not delete the information until advice is sought from an IT Security Manager. JobReady Live does not currently prevent or detect unaccredited information being introduced, or prevent a user deleting it. Providers are responsible for educating their staff as to what should be stored in JobReady Live and that they are not to delete information until advice has been sought internally.

- When information is introduced onto a system not accredited to handle the information, personnel should not copy, print or email the information. JobReady Live does not currently prevent or detect unaccredited information being introduced, or prevent a user copying, printing or emailing it. Providers are responsible for educating their staff as to what should be stored in JobReady Live and that they are not to copy, print or email it.

- Providers are responsible for the timely removal of JobReady Live access when their staff no longer require it and ensuring internal policies cover password management.
- Application logs held within the database will not be retained by JobReady following termination of a provider's contract with JobReady. It is the provider's responsibility to obtain a copy of the database prior to termination of their contract and retain as necessary to meet requirements.
- JobReady Live salts and hashes stored passwords using bcrypt according to industry best practices and OWASP ASVS guidelines. The bcrypt password hashing algorithm is not recognised as an ASD Approved Cryptographic Algorithm.
- JobReady Live provides Single Sign On (SSO) capability. It is the provider's responsibility to ensure this is enabled and configured, with multi-factor authentication enabled in the SSO Identity Provider. Recommended methods for managing Access Control within JobReady Live are part of the Consumer Guide. JobReady will work with providers to integrate with their identity provider and MFA capability.
- JobReady Live provides a customisable logon banner capability. Providers are responsible for setting the text in line with their contractual requirements.

Other considerations

The confidentiality, integrity and availability of database systems and their content is reported to be the responsibility of the provider as JobReady staff do not have visibility of the data stored within JobReady Live. The impact of this is that each provider is responsible to implement controls relating to how the database servers are accessed. Specifically:

> Control 1272: If only local access to a database system is required, networking functionality of DBMS software should be disabled or directed to listen solely to the localhost interface
>
> Control 1292: Agencies should verify the integrity of content where applicable, and block the content if verification fails
>
> Control 1294: When importing content to a security domain, including through a gateway, agencies should perform monthly audits of the imported content

The department does not understand this to be correct as the database administrators are JobReady staff and the import controls would typically be configured within the system, however JobReady have not had the audit report revised and resubmitted. Therefore each provider will need to work with JobReady to understand how to satisfy this obligation themselves before choosing to use JobReady Live.

JobReady response
A controlled set of privileged users do have access to the database and visibility of data within the database to support the administration of the service. Access is highly limited and subject to quarterly access review.

Similarly the ISM controls within the Working Off-site chapter were excluded on the basis that JobReady staff do not access the JobReady Live AWS environment through mobile devices. Therefore each provider will need to work with JobReady to understand how to meet the objective that information on mobile devices is protected from unauthorised disclosure before choosing to use JobReady Live.

JobReady response
Authorised JobReady staff can access the AWS environment from approved corporate devices over secure and encrypted channels. Sensitive information is not stored on staff devices.

The Strategies to Mitigate Cyber Security Incidents (the Essential Eight) is a prioritised list of mitigation strategies to assist organisations in protecting their systems against a range of adversaries, identified by the Australian Cyber Security Centre.

We note that JobReady Live resides in the AWS environment. JobReady staff are understood to have access to the system and the underlying databases containing job seeker data via their corporate-owned laptops. However, JobReady have elected not to have their corporate environment assessed as part of this accreditation. The audit report did not provide any results of testing in relation to the ACSC's Essential Eight mitigation strategies:

- Microsoft Office macro settings – as Microsoft Office is not used and web browsing functionality is not enabled in the JobReady Live AWS environment

- User application hardening – as the JobReady Live AWS environment does not have user applications.

Likewise, the methods to secure and manage the laptops and other corporate devices (such as servers, multifunction devices and mobile devices) then sanitise and securely destroy them were not assessed. The department can therefore not assess the risk to a provider's caseload by using JobReady Live nor has visibility of any continuous improvement plans JobReady may have. The department therefore recommends that each provider assesses this themselves before choosing to use JobReady Live. It may be appropriate to include clauses in your contract to prevent JobReady staff removing your job seeker data from the JobReady Live AWS environment, including via summarisation or benchmarking with other providers. A robust audit log review process would be required to identify if inappropriate data downloads took place.

JobReady response
Authorised JobReady staff can access the AWS environment from approved corporate devices over secure and encrypted channels. Sensitive information is not stored on staff devices.

Yours sincerely

Kerryn Kovacevic
21 October 2020