Australian Government

Department of Education, Skills and Employment

Accreditation of alffie's Learning Management System (LMS) third party employment system

This document is to assist employment services providers understand the scope of the accreditation of alffie's LMS performed for the Department of Education, Skills and Employment (the department). The accreditation assessment has been performed against the Information Security Manual (ISM) January 2020.

Accredited employment programs

alffie's LMS has been accredited for use to assist in the delivery of the following employment programs:

- jobactive
- Disability Employment Services
- Transition to Work
- Work for the Dole
- ParentsNext.

Accredited features and benefits

The following features and benefits of alffie have been accredited for use to assist in the delivery of the above employment programs:

Feature	Feature description
LMS – Learning Management System – Business Functions	- Provides Employment Service Providers (ESPs) with the ability to enrol participants, track outcomes and utilise alffie programs - Maintain file notes - Central place for participants to complete accredited courses - Track participant progress - Engagement with participants through SMS/ email (hosted wholly within Australia).
EPA – Employment Pathway App	Student case management application combining: - Skills testing - Job plan builder - Resume builder - Job seeker profile creation - Suggested careers and jobs.
Customised Engagement System	- Communication with participants and ESPs - Password resets - Certificates - Reports

Feature	Feature description
Reporting	Reporting is a key feature. All reports are highly customisable and exportable to multiple file types. These exports are available to users.
ParentsNext Application Module	This feature provides: - Creation of meetings for participant attendance requirements - Case notes - Non accredited/ accredited training.
Post Placement Support Module	This is a tool for an ESP to monitor a participant who has gained employment for the initial post placement period. This feature provides: - Enrolment into non accredited/ accredited training - Tracking of participants progress and required interventions.
Resume Builder	Allows users to create a resume using alffie course details and recommended skills.
Audit trail	alffie records audit logs covering actions by alffie staff, ESP staff or participants, such as: - Login activity - Course status - Internal and external user activity - Administrator user modifications - Documents accessed.
System security	alffie's systems and operations have been designed per Information Security Manual (ISM) January 2020 and is certified against ISO 27001:2013 customised to include the ISM controls. Current configuration includes
ESS Integration	LMS uses the department's ESS system to populate data relevant to participant's current status and employment journey, such as: - The participant's stream - Current requirements relevant to this status - Relevant documentation pertaining to contract status.
Bulk Upload of Participants	Allows drag and drop functionality to relevant reports to automate data addition and suggest next actions.
EC/Admin Dashboard Module	Gives providers access to the alffie system to view and generate reports covering all relevant users to track outcomes.
Search/Filtering Data	The reporting module allows for the filtering and searching of all data to allow the generation of adhoc reports.
Document Management	Allows the upload of documents relevant to participants.
Prospective Jobs Module	Allows participants to view jobs and allows Employment Consultants to track how many jobs have been received and viewed.
Noting	Provides ability to add notes to relevant participants.

Provider responsibilities

To use alffie's LMS 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 LMS.

- All interactions between alffie and the provider's ICT environment are subject to the provider's own assessment under the Right Fit For Risk assurance approach.

- alffie uses an extension of the shared responsibility model to deliver LMS. Amazon Web Services (AWS) is responsible for security **of** the cloud; alffie 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 LMS appropriately to meet their security requirements. alffie 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. alffie informs providers during implementation, and via ongoing training and support, of security requirements. will conduct regular security awareness training to providers to promote sound security practices in their configuration of alffie systems.

- 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 alffie access when their staff no longer require it.

- Forgotten passwords can be securely reset by each user using the Forgot password button on LMS. It is the provider's responsibility to positively identify users and maintain accurate contact information during enrolment or manual password resets.

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

- When using LMS there is a risk of a privacy breach if a provider staff member gives access to the incorrect participant, or if documents (e.g. a resume) were attached to the wrong record. There are no system controls available to prevent such a breach.

- When using alffie's messaging services, provider staff need to manually validate the participant's phone number. There is a risk of a privacy breach if a provider staff member enters the wrong participant's phone number. There are no system controls available to prevent such a breach.

- Data imported (exported) to LMS is not immediately scanned for malicious and active content. LMS will accept the importation of files in pdf, doc, docx, xlsx, xls, csv, png and jpeg file types. Attachments are uploaded into an S3 bucket for document storage, where there is no execution. Where a file cannot be scanned by alffie, the user is not 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 participants using LMS 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 alffie staff importing (exporting) content to LMS relating to their participants.

- 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. alffie 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 alffie 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. alffie does not currently prevent or detect unaccredited information introduced, or prevent a user copying, printing or emailing it. Providers are responsible for educating their staff as to what should be stored in alffie and that they are to pay particular attention to avoid data spillage/ leak when copying, printing or emailing.

- Application logs held within the database will not be retained by alffie following termination of a provider's contract with alffie. It is the provider's responsibility to obtain a copy of the database prior to the termination of their contract and retain as necessary to meet requirements.

- Providers are responsible for the timely removal of LMS access when their staff no longer require it and ensuring internal policies cover password management.

Action plans to address weaknesses

We note that LMS resides in the AWS environment.

As part alffie's continuous improvement, they have committed to raising the level of maturity in the areas of the Essential Eight and network security of their corporate network. This includes ongoing cyber security awareness sessions with staff and internal audits to validate that the controls they have in place continue to operate effectively.

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.

alffie will provide the department with the results of an independent assessment to support this has been achieved in the form of their ongoing customised ISO 27001 surveillance audit reports.

Yours sincerely

Kerryn Kovacevic   30/6/21
First Assistant Secretary – Digital Solutions Division

June 2021