Australian Government
Department of Education, Skills and Employment

Accreditation of Verner-Mackay Group's aXcelerate third party student management system

Verner-Mackay Group's third-party student management system, aXcelerate has been accredited by the Department of Education, Skills and Employment (the department) under the department's Right Fit For Risk (RFFR) program for the use in the provision of Australian Government services relating to registered training organisations (RTOs). This accreditation letter summarises the key RFFR matters, of which current and intended users of aXcelerate should be aware. This summary should be used to assist users, and potential users, of aXcelerate to determine the actions that they must take and the shared responsibility actions for which they are responsible when procuring and utilising aXcelerate in their business operations. The accreditation assessment was performed with reference to the Australian Government Information Security Manual (ISM) as of June 2021.

Accredited programs

Verner-Mackay Group's aXcelerate has been accredited for use to assist in the delivery of the following Australian Government skills and training programs:

- Careers Transition Assistance Program (CTAP)
- Employment Skills Training Services (EST)
- Skills for Education and Employment Program (SEE)
- Trades Recognition Australia (TRA)

Accredited scope of services

aXcelerate assists users with student management with features designed specifically for RTOs. It uses Amazon Web Services (AWS) to store and process data relating to students. The platform includes:

- Contract management
- Student management
- Trainer management
- Assessment delivery and management
- Compliance reporting
- General reporting
- Finance and eCommerce
- Automated workflows

Internal systems used by Verner-Mackay Group to support aXcelerate have not been included in the scope of the accreditation. The accreditation is limited to the aXcelerate service offered by Verner-Mackay. The accreditation has placed reliance on assertions by AWS with respect to the Australian instances of AWS and depends on the on-going conformance of the Australian instances of AWS with the requirements of the ISM.

Verner-Mackay Group's responsibilities with respect to aXcelerate

Verner-Mackay Group maintains the responsibility to provide secure code for the aXcelerate application through their ongoing development of the platform. Verner-Mackay will maintain the infrastructure and secure it through the regular auditing of security controls.

Verner-Mackay Group's infrastructure partner for aXcelerate, AWS, provides physical and virtual security for the operating environment and network infrastructure, while maintaining availability for end users.

Verner-Mackay Group provides training to their customers so that they have the requisite skills for administration and configuration of their instance of aXcelerate. This training includes teaching customers in the configuration of privacy and security settings in aXcelerate. While Verner-Mackay Group trains new customers, it is the customer's responsibility to transfer knowledge when the administrators at customer organisations move to new roles. Verner-Mackay can provide assistance to retrain if necessary.

Customer responsibilities

When an RTO provider (the Customer) implements aXcelerate as part of their IT environment to deliver services to students and apprentices, the provider retains accountability and responsibility for conformance with provider requirements with respect to RFFR.

- Customers are to advise the department of their intention to start, expand or cease using aXcelerate.
- All interactions between aXcelerate and the Customer's ICT environment are subject to the customer's own assessment under the RFFR assurance approach.
- Customers are responsible for managing users within the system, both administrative and student users. This includes removing outdated data from users that are no longer current within the organisation.
- Customers are responsible for configuring system role profiles based on the principle of least privilege.
- Customers should ensure system users are using passwords that are unique to aXcelerate and not used for any other system.
- Customers should ensure each system login can only be accessed by a single individual and that credentials such as usernames and passwords are never shared between users.
- Customers are responsible for enabling multi-factor authentication for all administrative users of aXcelerate.
- Customers are responsible for enabling multi-factor authentication for general users wherever possible.
- Customers are responsible for implementing controls to limit access to sensitive data stored in aXcelerate according to the 'need to know' principle.
- Customers are to maintain a secure IT environment within their organisation that includes secure controls on network access, both internally and externally.

- Customers are to notify Verner-Mackay Group immediately upon identification of a security breach. This includes unauthorised user access, disclosure or dissemination of private information, user account compromise, or any other event that statutes a risk to either the end user or aXcelerate.
- Customers are to maintain a secure computing environment that ensures the end user's devices are free from malicious software such as viruses and malware. This includes implementing the ACSC's Essential Eight strategies to mitigate cyber security incidents on Provider endpoint devices as relevant.
- Customers are responsible for API keys rotation and that the API keys are not disclosed to any unauthorised or untrusted parties. Like regular users, the security permission profile of an API user account should be based on the principle of least privilege.
- Customers are responsible for performing appropriate security audits on any third party that would be issued an API key for development purposes.

Action plans to address weaknesses

The ISO 27001 Stage 2 report (adopting the DESE Scheme) noted 55 controls **were not operating as designed** and were listed as opportunities for improvement. Verner-Mackay Group, as part of their maintenance of their RFFR accreditation, are required to keep the department informed of the actions being taken to address the opportunities for improvement. This includes, but is not limited to:

a) Advising upon completion of actions relating to the implementation of the essential eight controls on the Apple Macintosh computers used to administer the AWS relational database system.

b) Advising upon completion of actions relating to other items on the Action Plan.

c) Quarterly conference calls with the department to provide updates on progress of on-going information security improvements. Where there is a significant change to the security of the environment assessed, Verner-Mackay Group must:

i. notify the department of the nature and scope of the change.
ii. provide an assessment of the impact of the change.
iii. confirm the documented ISMS and procedures has been or will be updated because of the change; and
iv. confirm procedures are implemented effectively.

Verner-Mackay Group will provide the department with the results of an independent assessment, through their ongoing annual customised ISO 27001 surveillance audit reports, to confirm that the identified weaknesses have been addressed.

Yours sincerely

Kerryn Kovacevic
First Assistant Secretary – Digital Solutions Division
19 April 2022