aXcelerate Security & Data Management

Information Classification

Public

Version Control

Name	Version	Date	Comments
Nathan Gordon	0.0.1	31/10/2012	Initial Draft
Tien-wei Lin	1.0.1	09/08/2013	Update to The Current Security Mechanism
Michael Ryan	1.0.2	25/09/2013	More detailed explanation of security measures.
Reay Mackay	1.0.3	15/02/2014	Update with Amazon Web Services network diagrams
Michael Ryan	1.0.4	12/03/2014	Added release cycle information and application/database redundancy and recovery information. Some diagrams removed.
Michael Ryan	1.0.5	11/06/2015	Added disaster recovery details around recovery times and disaster scenarios
Jade Steffensen	1.0.6	11/12/2015	Added clarification around client data segregation assurance.
Michael Ryan	2.0.0	15/03/2016	Documentation of major updates to aXcelerate infrastructure. Major change is move from AWS RDS to AWS EC2
Michael Ryan	2.1.0	12/10/2018	Monitoring information added
Michael Ryan	2.1.1	04/12/2018	Data breach information added
Jacob Lehr	2.1.2	21/02/2019	Updated systems information
Michael Ryan	2.1.3	20/09/2019	Clarification on AWS infrastructure. Single-tenancy option
Josh Cannons	3.0.0	07/09/2022	Major document refactor to include new security developments, clustered infrastructure and migration to RDS for databases. Layout changes for clarity.
Josh Cannons	3.0.1	08/11/2023	Updates to backup schedules.

Introduction

This document explains both the functionality and technology behind the security of the aXcelerate application and the control and development processes involved with developing and deploying the application.

From a functional perspective, aXcelerate houses its data behind a login secure web application that manages session data and combines role-based and permission-based security in all areas of the system. Data partitions for each aXcelerate account can optionally be broken down further into Domains.

From a technical perspective, this document explains how the application secures sessions, the security of the infrastructure that hosts the application, the redundancy of our systems and our system processes to prevent any internal or external vulnerability.

Infrastructure

AWS

Amazon Web Services (AWS)[1] is a world-class leader in cloud services. AWS was chosen because it will allow the application to horizontally and vertically scale with the greatest ease. We are currently using multiple services within the AWS ecosystem including EC2 instances for our application and infrastructure servers, Route 53 domain name service, Application Load Balancers to ensure performance and server scaling, Simple Storage Service (S3) Storage, Web Application Firewall (WAF) for request filtering, IAM access and security controls and Relational Database Service (RDS) for all our databases. All aXcelerate data is securely and exclusively stored in Amazon's "Asia Pacific - Sydney" Region[2] to ensure compliance with data sovereignty regulations.

Amazon Web Services infrastructure complies with the most stringent international standards which is why this platform was chosen to host aXcelerate[3]. Amazon is an ISO27001 Compliant SOC 1/2/3 provider.

The move to the Amazon Cloud has provided the following key benefits:

1. Ability to scale the application easily and quickly as new users are added or peak workloads are experienced. Spawning a new Amazon server takes a matter of seconds/minutes not hours/days. This translates to higher application performance for end users during normal and peak workloads
2. Data durability has increased significantly (Amazon's 11 9's data durability is industry-leading) meaning our clients can rest easy that their data is being backed up in several locations and the risk of data loss is eliminated.
3. Data security has increased significantly with Amazon's unique Multi-Availability Zone (MAZ) deployment with data continuously being backed up and stored in multiple geographic zones that are unknown even to Amazon employees providing even greater peace of mind for our clients and their data.
4. Associated server infrastructure such as the goFlow Workflow Automation server, Moodle server and email servers can all be managed from the one control point enabling greater application integration and reduced cost which ultimately flows through to our clients.

aXcelerate has deployed a vast array of servers to support the application, each with its own specific purpose. aXcelerate's production servers can be hosted in any of three Availability Zones in the AWS Asia Pacific Sydney Region - ap-southeast-2. Where practical, server instances that frequently communicate with other servers, e.g the main application web servers and the production database server, are all housed within the same Availability Zone to ensure high network speeds. Data redundancy is shared across all Availability

[1] You can learn more about AWS at aws.amazon.com.
[2] AWS Regions and Availability Zones
[3] Details of Amazon's compliance can be viewed here

Zones in Sydney and if any zone becomes unavailable, the affected servers can be rebooted from Amazon Machine Images (AMIs) within minutes.

aXcelerate uses a clustered multi-tenanted data model which means clients are separated into shared clusters with data from each cluster stored within its own database. The data within these databases are separated with a combination of public and private key fields on all primary data entities which creates a virtual partition between the data in each account. This increases our scalability potential and also provides additional security provisions. There is also a single-tenancy option for clients who wish to have a physical partition between their data and other clients' data. This option will have fees attached for running additional servers in AWS.

Data within our infrastructure is encrypted at rest via Amazon Key Management Service (KMS) using 256-bit AES-GCM symmetric encryption. All aXcelerate data is encrypted in transit and delivered over SSL via TLS 1.2. This ensures our security and data authenticity is always maintained.

Access to infrastructure management is restricted to only a few trusted engineering team members and is also hardened with complex password requirements[4] and multi-factor authentication (MFA) using a secure token. Additionally, server access is limited via Public Key authentication using a hardened SSH configuration. At no stage are shared credentials used for access.

Database

We use high-performance Microsoft SQL Server instances hosted via Amazon Relational Database Service (RDS) for our application. These database instances use memory-optimised managed instances to ensure a high level of throughput without bottlenecks.

All our database server instances are protected by AWS Security Groups which is a stateful firewall service for resources with the AWS data centres. Policy rules are created for different server groups to harden the security of all infrastructure and limit traffic between the infrastructure to authorised networks. For instance, application web servers are open to public access on port 443 to enable secure requests from a user's web browser, but access to the databases is limited to the application servers and management IP addresses.

The security of our databases is treated with the utmost importance. As such all data is encrypted within the databases using built-in AWS encryption methods and managed by AWS Key Management Service.

[4] AWS Access Password Policy is as follows;
Minimum password length is 14 characters
Require at least one uppercase letter from Latin alphabet (A-Z)
Require at least one lowercase letter from Latin alphabet (a-z)
Require at least one number
Require at least one non-alphanumeric character (! @ # $ % ^ & * ( ) _ + - = [ ] { } | ')
Allow users to change their own password
Remember last 24 password(s) and prevent reuse

Database queries are protected from SQL injection at multiple levels. The data source connection configured on the application platform does not have any privileges to execute CREATE, ALTER, DROP or GRANT statements.

Our development standards also dictate strict parameterization so any values submitted via HTML forms or embedded in a URL are type-checked and cannot execute additional SQL statements. All user passwords are hash encrypted with a secret salt. This means that our passwords have one-way encryption and cannot be decrypted by anyone, including us. This prevents anyone from ever being able to read our passwords from our database, even if using a hash-matching database. A similar algorithm is used to store Tax File Numbers for VET Student Loans enrollments. aXcelerate does not store any credit card details within the application.

While other Personally Identifiable Information (PII) within the application such as Date of Birth, Address, Email Address and USI are not encrypted within the database, the database itself is encrypted as are the snapshots and backups of the database.

Application

Framework

aXcelerate is a multi-tenanted database application powered by MSSQL Server databases as well as some other MySQL databases for some specific features. The application runs on Ubuntu servers with a Java application. The aXcelerate application itself runs on a combination of an open-source Cold Fusion Markup Language (CFML) platform called Lucee[5] and a Javascript framework developed by Microsoft called TypeScript[6].

Some features are built with pure Java libraries while the front-end has a combination of standard JavaScript, JQuery and React. We comply with HTML5, CSS and Javascript standards so that all functionality will work as intended with modern browsers.

The application utilises a variety of AWS services to improve performance and security;

1. AWS Cognito is used to define user authentication, define rules for complex passwords[7] and allow Single Sign On via Security Assertion Markup Language (SAML) providers that let clients sign on via their existing federated authentication servers. aXcelerate recommends using a SAML provider for better security
2. AWS Auto Scaling allows application servers to elasticity create new servers to meet incoming load
3. AWS Web Application Firewall (WAF) Monitors all incoming requests to the application and filters out malicious requests before they enter the system

Client Session & System Data

Within aXcelerate's database and codebase, client data is divided by a key system field. Each Client has a unique key that acts like a 'fingerprint' or 'marker' that is applied to records and files. On login, this 'fingerprint' is attached/related to the User. All requests made by the User require the key which is tracked by the server for the life of the session (while the User is logged in).

Strict segregation of client data is maintained through the checking of client unique keys at all levels of the application, internal database integrity constraints, locking down database access from external sources, and rigorous automated testing of all features that access client data. This ensures the highest level of data segregation and security.

On the public side (i.e. website integration - public booking): the unique Client key is embedded with each request.

[5] Lucee information can be found at https://www.lucee.org/
[6] TypeScript information can be found at https://www.typescriptlang.org/
[7] Axcelerate User Password policy is as follows;
Minimum length: 8
Must require uppercase, lowercase and a digit.

System data is used by all Clients and is generally only accessible/updatable by aXcelerate Administrators (Super Users) - This information is used by the aXcelerate application and may have business logic written against it. There is one exception to this rule: Global Course Search. As Clients add new qualifications, these courses are added to a global list of courses that are accessible by all Clients.

aXcelerate keeps several logs throughout the system to track User interactions that may need to be monitored or audited at a later date. Every time a User logs in, this information is stored with the I.P. address of the requesting connection. Similar logs are kept for accredited unit data, online transaction sessions, and system errors to name some examples. The logs are kept in a dedicated logging database hosted in Amazon RDS.

Default User Roles

There are currently several default types of User Roles in aXcelerate. Each role has a default set of permissions assigned to them. In addition, aXcelerate provides the capability of creating custom roles assigned specific permissions simply by ticking the checkboxes as well as assigning a specific portal for the role.

From highest to the lowest level of access:

1. Administrator
2. Admin Support
3. Trainer
4. Student

Administrator: Should have complete control over the system (all boxes selected). The system will always ensure that there is at least one Administrator.

Admin Support: Should have partial control of system functions (mostly view and update permissions). Users with this role are supposed to assist Administrators to deal with nontrivial tasks.

Trainer: Functionality to display different information on a Trainer Portal. This will include quick access links specific to a Trainer role and information regarding recent and upcoming courses that the Trainer is delivering. Users with this access level may not appear on some user-related drop-down lists.

Student: Functionality to add/modify their own contact details, enrol in courses available, complete assessments assigned to them, view their own current course completions and similar student functions.

aXcelerate also offers the flexibility of editing User Roles to alter permissions. Furthermore, except for the Administrator Role, the rest of the User Roles are deletable.

User Creation

When creating a User (from a Contact record) you are able to select one of the User Roles including customised roles and accept the specific permissions based on the selected User Role. Alternatively, the System Administrator can override the default role permissions for a specific user. What is more, all Existing Users can be searched by entering keywords and can be activated/deactivated by clicking the de/activate icons. You can also sort by Username or Access level.

Override Permissions

A User with the permission setting of ‘User Management’ can edit the Access Level in terms of changing a different User Role and customising permissions (Highlighted Spots on the sample image below). Additionally, when clicking the Reset Password button, the system will send an email with a link to facilitate a password reset.

Domains

Domains within the application are an optional feature. A Domain is a security and reporting option that creates groups of users that can see their domain's data. A Domain could be 'Marketing' or 'Northern Region' or 'Queensland sub-branch'. You can create whatever Domains might apply to your operating environment and business needs. Nesting of domains is not currently supported by aXcelerate.

Backup and Disaster Recovery

Codebase

The aXcelerate codebase backup and versioning are managed internally but located externally in Atlassian Bitbucket. Bitbucket is an enterprise-grade, GIT repository which has been trusted by over 450,000 teams and 3,000,000 developers around the world. Each release version of aXcelerate is saved as a snapshot within our GIT repository and has multiple redundancies.

All code changes experience extensive and isolated testing in development, testing and staging environments by a dedicated QA team before code is pushed into our production system. All members of our development team frequently participate in code reviews as an added measure to prevent any unwanted or speculative code from becoming part of the application.

Code changes are controlled via Atlassian Jira, an issue tracking system that ties into BitBucket and tracks Bug Tracking, Change Management and Project Planning. Within Jira, all changes are assessed for impacts on Information Security Risk and our QA team provides feedback after testing any possible risk.

Client Resources and Files

aXcelerate files are currently stored securely within Amazon's S3 (Simple Storage Service) which is proclaimed as having 'eleven nines of durability (99.999999999%) making it one of the most secure and reliable storage sites on the planet.

Database

For the aXcelerate database requirements, we utilise a single database for each shard hosted in AWS RDS. A centralised backup policy managed in AWS backup ensures backup compliance across all aXcelerate databases. We perform a full database snapshot every 12 hours and back up the transaction log every 5 minutes. This allows a backup Recovery Point Objective (RPO) of 5 minutes. Backups of the database are stored for 7 days within the AWS infrastructure. In addition, we perform monthly database backups that are stored for 7 years at present.

In the event of a complete failure or corruption of our primary database server, several aXcelerate employees are capable of carrying out our DR (Disaster Recovery) procedures to restore the database to any point in time no more than 5 minutes before the disaster occurred. This event does result in some downtime of the aXcelerate application to allow for a SQL server backup restoration and reconfiguring of the application to direct database requests to the new location. This time would be minimised due to this infrastructure already being in place and our expected Recovery Time Objective (RTO) for a database recovery

procedure is under an hour. Database recovery procedures are performed and recorded annually at present.

Application

As part of the release cycle outlined below, an aXcelerate application server is created from an image known as an Amazon Machine Image (AMI) ensuring consistency and management from a single Standard Operating Environment (SOE). Application server clusters are created using Infrastructure-As-Code using AWS Cloud Formation templates stored securely within our git repository. The templates define everything from Instance type, security management and Auto-Scaling capabilities. Using these templates in conjunction with the AMI, it is possible to create an entirely new Axcelerate cluster within minutes.

Due to the static nature of an AMI, it is easy to scale up any number of server instances and add them to the load balancer to support the volumes of traffic required to keep aXcelerate stable and responsive. These servers are split between the EC2 Availability Zones in Sydney and additional server instances can be added at any time to support extra activity. During peak AVETMISS/other reporting periods, (usually the last five working days in each month). In the event of any server supporting the application stalls or becomes unstable, the server can be removed from our load balancer and additional servers can be added within 5-10 minutes.

Outage and Disaster Recovery Scenario Responses

Single application server outage - This scenario would usually **have no impact on an end user** due to our server redundancy and dynamic load balancing. In the unlikely event that a user was currently awaiting a request and the load balancer had directed that request to the affected server at the time of the outage, the page request would time out and the user may have to click back or refresh in the browser to continue working.

Multiple application servers simultaneous outage during business hours - The user is **not likely to be impacted** by this event. In this scenario, our load balancer would direct all traffic to the remaining available web servers. The result is basically the same as per the single server outage however if the outage affects a significant number of servers, end users **may experience slightly slower response times** until servers are restarted or new servers are added to the load balancer. This usually takes an aXcelerate systems administrator **between 5 -10 minutes** to carry out this procedure.

All application servers simultaneous outage - In this scenario, all servers have to be removed from the load balancer and restarted before being added back to the load balancer. Again, this would take a systems administrator **between 5 - 10 minutes** to bring servers back online. **The user would not be able to use aXcelerate during this time.** Upon servers restarting, users will be able to continue working without having to log in again. It is highly unlikely that All web servers will fail at the same time due to the fact that the load balancer will detect individual failures and automatically begin to correct the issue.

Application server outage outside of business hours - SMS notification systems have been set up to inform aXcelerate systems administrators and developers if this occurs **within the hour**. In this event, the administrators have the ability to add new functioning servers to the load balancer. This procedure will take between 5 - 10 minutes but usually, our server redundancy prevents any impacts on end users as the load balancers can automatically correct the issue.

Database locking or slowness - This can cause the aXcelerate application to have intermittent periods of slow response times for any length of time **between one minute and up to several hours**. Altering has been set up to alert the Database Administrator and Infrastructure staff that performance has been affected. These alerts include high CPU load, database deadlocks and Load Balancer response time.

In most cases, locks can be cleared by a database administrator within a couple of minutes and the application performance would resume as normal. In some extreme cases, a page request may trigger a database query that has a negative impact on the database. The danger in this extreme case is that the user may run this page request several times. In this scenario, all available aXcelerate developers would investigate this as a matter of urgency to resolve it as soon as possible. The offending SQL query can be identified through our monitoring tools and it is quickly determined if a piece of code needs to be hot fixed or if the database requires tuning. This usually takes **less than thirty minutes** and users may experience intermittent slowness during this period. If a feature needs to be disabled to prevent this from repeatedly occurring this will be hot fixed as soon as possible before a more permanent solution is found. In the past 12 months, this type of scenario has occurred only twice.

Database server outage - In this scenario, the aXcelerate application will not be accessible. Our database servers are managed instances on redundant hardware offering a significant uptime ratio of 99.95%[8]. In the advent of a database outage, it will be required to restart the database instance. This will result in a downtime of approximately 5 - 10 minutes while the instance restarts.
If it is determined that there is an issue with the AWS data centre, aXcelerate may make the decision to deploy the latest backup to another available AWS data centre and the aXcelerate application can be recovered in approximately two hours. This would result in data loss of up to five minutes before the crash occurred, so the preference would be to restart the instance and allow the primary database to come back online.

[8] AWS RDS Service Level Agreement https://aws.amazon.com/rds/sla/

Development/Release Cycle

General Guidelines

aXcelerate development is a continual process with ongoing advancements in the functionality of the application. To ensure the process is free of bugs, we undergo multiple levels of testing and evaluation. Initial development is committed to our testing environment, an internal-only version of our application that undergoes constant testing from a dedicated Quality Assurance (QA) team. Once code passes testing it is committed to our Staging environment. This is where the code undergoes further testing from QA, along with client interaction. This allows for a greater level of testing in real-world environments. Only after code has been tested in Staging can it be committed to the main Production account and released to the public as the aXcelerate application.

Each change is reviewed for any application or information security risk. Any identified risk is then tested by the QA team and monitored by Staff in Sentry, our bug tracking system.

The development team avoids making major environmental changes at the same time as a release because there is increased risk and it is more difficult to determine if an issue is a result of code or a configuration setting.

In general, We aim for a fortnightly release schedule to ensure our application is kept as up-to-date as possible.

The fortnightly release cycle is supported by the following processes and procedures:

Tuesday (The day before Production release)

- Check that the help documentation has been updated for new features in the upcoming release.
- The tasks system should be reviewed to ensure that all code changes going into the upcoming release have been tested.

Wednesday (The day of Production release) - Production release

- Confirm with QA/Jira that all testing has been completed
- Discuss release with developers
- Push the current Staging branch to the Master branch
- AWS Code Deploy will now begin deploying code to the production servers one at a time
- Review Sentry for any issues

Thursday (The day after Production release) - Risk Assessment and Code Stability.

- Continue reviewing Sentry and perform post-release performance reviews
- Using Thursday/Friday as buffer days before creating the next Staging code branch allows us to resolve any new bugs discovered in production after the release.

Tuesday (The week following Production release) - New Staging Branch and Update Staging

- The database changes log is locked down for the next release.
- Ensure all code reviews have been performed on upcoming changes to the Staging Branch
- Close off the Staging branch to stop any further changes from being committed
- Create a new pre-release Branch with the code from the closed staging branch
- The releaser and support team should re-prioritise the tasks list and allocate all the tasks to be completed in the next cycle.
- Check with the development team if any other scripts need to be run and append those to the release plan if necessary.
- The releaser should keep a local copy of the new branch and the previous one. The oldest copy can be switched to the new branch.
- Set AWS CodeDeploy to use the new pre-release staging branch
- Push the pre-release branch to git
- AWS Code Deploy will now begin deploying code to the staging servers one at a time
- Inform QA and being testing the Staging branch code

Security and Monitoring

aXcelerate has extensive monitoring and alerts set up to ensure a high level of uptime and responsiveness can be achieved. Each of the following tools or features has been implemented to allow us to report on trends and critically, to be able to notify aXcelerate staff when any feature of our infrastructure needs attention. After hours, any of the monitoring tools below can send text messages to the appropriate person so we have around the clock assurance of our systems.

Enterprise SIEM

aXcelerate implements a Security Information and Event Management (SIEM) system that collates logs from a variety of sources into a single interface for review. Data collected by the SIEM includes database logs, web server access logs, security scan results and AWS access and API usage. These logs are parsed by the SIEM which in turn uses industry-leading Indicators of Compromise (IOC) to identify any potential malicious activity.

A multitude of alerts have been set up that detect and report on a large array of results including requests from malicious IPs, external and internal attempts at malicious activity, security-related infrastructure changes and suspicious web requests. These alerts notify security staff as required.

AWS CloudTrail

AWS CloudTrail is a service that allows operational and risk auditing, governance, and compliance of all our AWS accounts. It records actions taken by a user, role, or an AWS service as events in the CloudTrail log. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs. We send all events in CloudTrail to our enterprise SIEM for further analysis which provides alerting and reporting on potentially suspicious events and allows for user action auditing within our infrastructure.

AWS CloudWatch

AWS Cloudwatch provides a log aggregation and system monitoring console for all services within AWS. We have a multitude of alerts in AWS Cloudwatch to alert us when there may be an issue causing the application to slow down, become out of service or require additional manual review. These alerts include checks for consistent high CPU usage or when servers run out of memory and drop off the load balancer. Cloudwatch load-balancer reporting allows confirmation that our main web servers are performing well.
In addition, a selection of application and database logs are sent from the clusters to CloudWatch to provide a single point of management and collation.

AWS GuardDuty

GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorised behaviour within our AWS accounts, EC2 servers and data stored in Amazon S3. GuardDuty combines machine learning, anomaly detection, network monitoring, and malicious file discovery to identify unusual activity within the infrastructure. It further analyses the security relevance of the activity and gives the context in which it was invoked.

AWS Guard Duty will send an alert to security staff if anything is found that warrants investigation. This allows us to determine if the incident is a false positive or if we should spend time on further investigation and remediation. Additionally, all the incidents are logged within our CloudWatch logs and sent to the network SIEM for additional review.

Nagios

Nagios is an open-source industry standard monitoring tool with enormous capabilities. We have configured Nagios to monitor drive space, memory, CPU usage and many other internal attributes of all our servers. This provides a monitoring solution external to AWS CloudWatch to ensure redundant monitoring is happening across the system.

Fusion Reactor

Fusion reactor gives us a high level of detail about exactly what happens inside the Java Virtual Machine (JVM) of our main web servers. It is present on all application servers and records web and database metrics from the requests made by clients. If there is a slow request, FusionReactor enables us to see exactly what the bottleneck is, whether it be database blocks, low memory or anything else.

SQL Beacon

This tool is authored by a Microsoft Gold partner and provides daily reports about the health of our SQL Servers. This can help us identify any future problems with the application before they arise and show us if any parts of the database require tuning.

Data Breach Incident Response

In the event of any security or data breach, aXcelerate will follow procedures to notify all staff and any/all affected clients immediately. Also, in accordance with the Australian Privacy Act 1988 as outlined by the Office of the Australian Information Commissioner (OAIC), any breach that could be classified as a Notifiable Breach will be reported appropriately.

FAQs

1.0 - Architecture and technologies

1.1 - Where will the product be hosted? Private or Public cloud?

Public Cloud (AWS Sydney) only.

1.2 - Is the product multi-tenant or single-tenant?

Multi-tenanted is the default. Single is available for an additional cost.

1.3 - Our training organisation often experiences peaks in demand. Are there any known limitations? Please describe how the product has been built to scale.

aXcelerate is built to be able to quickly add additional application servers to our load balancer where necessary. We have maintained a highly available system that currently supports up to 500,000 requests per hour with low latency.
Each cluster has its own database to reduce the load on the database ensuring each performance. The databases run on memory-optimised managed instances hosted in AWS RDS.

1.4 - What is the availability of the product in terms of percentage? Describe how you achieve high availability. Describe the redundant components of the architecture and the failover mechanism.

We have delivered close to 99.99% uptime over the last 12 months (not including scheduled maintenance). We have highly tuned databases and flexible load balancers for the main application. Reporting is done by a separate data warehouse. The application is written with scalability in mind so we can accommodate high-volume traffic.

1.5 - Do you have an asset management policy in place which contains an inventory system for hardware and software assets?

The AWS Console provides an asset register for all hardware required to support the application. Any resource can be ‘tagged’ to categorise it as being for testing, staging, or production environments, the general role and other tags as required.

Internally within the office, HR is responsible for keeping the hardware asset register for all onsite hardware in use by aXcelerate employees. Most software we use is SaaS delivered through a browser, e.g. Gmail, Asana, Jira, Zendesk and our licence register is managed by our accounts team through Xero. Additionally, Jamf Apple device management tracks all software installed on developer machines

1.6 - Does aXcelerate support network communication protocols (i.e., RDP/HTTPS for remote management, Syslog, SNMP, NTP, FTP)?

The aXcelerate production environment (both browser and APIs) is only accessible through HTTPS.

Other network communication protocols are not used.

2.0 - Data protection

2.1 - Is there a plan in place to ensure that access to our data is limited to only your essential staff?

The aXcelerate staff are only given access to the systems that they need to fulfil their job requirements. For the majority of our staff, this includes the ability to impersonate aXcelerate users from all client accounts so we can support and assist users. All impersonate access is logged within a protected database.
All our staff are trusted and bound by contract not to possess or expose any client confidential information.

2.2 - How will data be protected within your Data Centre, system, backups and any endpoint devices?

Direct access to all data and systems are protected by 4 levels of authentication:

- AWS Security Groups (Network Firewall)
- Web Application Firewall
- AWS Guard Duty (Malicious activity monitoring)
- Individual security certificates for root access to servers
- Enforced MFA when logging into to the AWS console
- Monitored SIEM reporting and alerting

Backups in AWS S3 have industry leading durability.

2.3 - Please describe the security controls in place to protect data. How are they monitored and managed?

In the application, Role Based Access Control (RBAC) privileges are applied through the application so that administrators control which users have access to the data. These are managed by the client.
Within the infrastructure, access also follows RBAC controls. Developers have limited access to the infrastructure of the testing environment to monitor code commits and build errors. System Administrators have greater access to the infrastructure used to monitor and manage the servers and services used to deploy and maintain the application and associated resources.
All access to the infrastructure is logged within AWS CloudTrail and sent to the SIEM for review. In addition, quarterly access audits review all users' access to the infrastructure for unnecessary or unused controls.

2.4 - What certifications does your company have?

We are ISO27001, ISO9001, DESE and RFFR compliant, which an authorised third-party audits annually.

2.5 - What advanced attack detection/prevention capabilities exist to protect data in your Data Centres?

AWS Shared responsibility model[9] incorporates the strength of their advanced network and security features with our AWS Well-architected approach to security. This is in addition to the controls mentioned previously in this document.

2.6 - Does the product encrypt data at rest and in motion? Describe the methods & protocols used. (SSL, TLS 1.2 etc.)

Currently, all data is encrypted within the database and application using AWS Key Management Service (KMS). This uses 256bit AES-GCM encryption.
aXcelerate is only available over SSL with a minimum of TLS 1.3

2.7 - Will aXcelerate process information that will be considered sensitive (i.e., PII, PCI)?

The aXcelerate software processes PII and related training records of individuals. This data is saved to encrypted MSSQL databases hosted in AWS RDS in the Sydney datacentre. PCI data may be processed through secure and encrypted web interfaces but this data is not stored in aXcelerate.

2.8 - Does aXcelerate process information that is classified as 'restricted' or 'confidential'?

aXcelerate stores some confidential information against individual records such as TFNs for students requiring VET Student Loans. Sensitive data such as this, and also security-related data such as passwords, are persisted as encrypted records in the database.

2.9 - When providing support, where are the support staff accessing the data from?

All our support staff are based in our Brisbane office. We have other Australia-based sales and onboarding staff that will assist when necessary from off-site locations within Australia. We have no overseas support staff accessing client data.

2.10 - Does aXcelerate require remote access from the vendor for implementation & ongoing support? How will it be achieved securely?

Because aXcelerate is a web application, support can be provided through an impersonation feature built into the software. This feature eliminates the need to have remote access type protocols.

3.0 - Data Storage and Recovery

3.1 - What information will be stored in this application / or hosting facilities?

Student data and assessment data, as well as all the data required to manage the logistics of training management and fulfil government reporting compliance requirements.

[9] https://aws.amazon.com/compliance/shared-responsibility-model/

3.2 - What is the classification of data being stored in this application / or hosting facilities?

The most confidential data is student data (PII data) and training data which contains progress and completions of training courses. Also, financial data relating to invoices and payments for training. All other data would be classified as non-confidential

3.3 - How long will data be retained?

As long as you stay with aXcelerate.

3.4 - Can you share where the cloud data is stored? Is it stored in an overseas location?

Our data is stored in the AWS data centres in Sydney. For added security, the exact locations are not published by AWS. Our data is also backed up in AWS S3[10].

3.5 - What are your archiving and destruction practices? Please explain your procedure for physical destruction of disks, and data deletion using secure erase tools.

Physical:
Within the office, we have a general “Paperless Office policy” where required. All paperwork that is no longer required is shredded. The Data destruction procedure of physical media is defined within our Internal Clean Desk Policy and additionally within our Information Security Management Policy.

Electronic:
For data in the AWS Data Centre - once deleted, data is no longer available. Client data can be deleted from AWS by request. If multi-tenanted, database data is obfuscated if a client leaves. Historic Backups are kept and not tampered with. AWS S3 allows us to create lifecycle policies on information such as database backups. We configure these rules to reflect our data retention policy as per our terms[11].
Client data is not stored electronically on the office premises.

3.6 - Does aXcelerate have data leakage/loss protection features at the host ry level?

Data loss can only occur at the database level. The database has an extensive backup history and there are many change log features for critical areas of the application. Files (assessments, certificates, etc.) are stored within Amazon S3 with “11 9s of durability”.

3.7 - Please describe the application backup and restore procedures.

The application database transaction log is automatically backed up every 5 minutes. The database restore procedure is documented and this procedure is tested at least once per year in a test environment to ensure our team can recover from a system failure quickly and precisely.

[10] https://aws.amazon.com/s3/faqs/#data-protection
[11] https://www.axcelerate.com.au/terms/

3.8 - What is the Recovery Time Objective (RTO)?

Where AWS ap-southeast region resources are still available, our database recovery procedure has a 1-hour RTO, with additional time dedicated to testing and operational recovery giving an estimated operational RTO of 2 hours.

3.9 - What is the Recovery Point Objective (RPO)?

Our recovery point objective (the time elapsed between system failure and the last data backup save point) is approximately 5 minutes.

3.10 - Does aXcelerate support data protection during storage (at rest), processing (in use) and transmission (in transit)?

Data at rest has extensive protection that includes backup and encryption. Transactional data changes are utilised where necessary and development standards dictate strict use of database constraints where applicable to ensure data integrity. aXcelerate is only accessible via HTTPS, so data is also encrypted in transit.

3.11 - We might have legal obligations to keep our data inside Australian borders. Please describe how your product meets this requirement.

We only use AWS resources based in Sydney. No data is stored overseas

3.12 - Is there a 'Business Continuity Program' (BCP) and Disaster Recovery Plan (DRP) in place?

Our Business Continuity Program relies on the backup and safekeeping of our production code and database. Our database transaction log is backed-up every 5 minutes and a database snapshot is taken every 12 hours. Database backups are managed through AWS backup service and hosted within the infrastructure itself.
Our code is copied locally onto all our developer machines in our office and all commits are made to a cloud-based repository.
We have a Disaster Recovery Plan that has been practised and verified. Database backups can be quickly restored and our application servers can be deployed from Amazon Machine Images (AMIs) to any of three (3) data centres in Australia.

3.13 - If using a shared instance of a database, how will the data be separated from your other customers?

Virtual separation through keys linked to records on the database. Any user record is linked with the key and will only be able to access data with the same key. Single-tenant instances are also available, offering dedicated database and server instances.

4.0 - User management

4.1 - Does aXcelerate support user authentication (i.e., Multi-Factor, Biometrics, Local DB, AD, LDAP)?

aXcelerate natively supports Password Access Authentication. The application also allows for Multi-Factor Authentication (MFA) although this is not enforced through the application.

aXcelerate does provide API endpoints that are capable of generating security tokens to support Single Sign On (SSO) if the client wishes to integrate in this way. aXcelerate recommends using the SSO option if it is available to ensure greater security and management of access. It does not natively support any other authentication methods.

4.2 - What are the password reset protocols?

aXcelerate customers with Administrator privileges have control over resetting passwords for their accounts. Users can also individually use our reset password mechanism.

4.3 - Does the product save passwords? Describe the security controls relevant to password protection.

User passwords are saved within the database to allow authentication. Passwords are encrypted using One-way encryption meaning aXcelerate cannot decrypt or view passwords. If passwords are forgotten they must be reset. A user can do this or an administrator can force reset a password to be emailed to a user.

4.4 - Does aXcelerate segregate user roles/ functions and manage user privileges (i.e. RBAC feature, integrate with PAM systems)?

Yes. aXcelerate has role and domain-based access controls combined with individual permissions for user functionality within the system. This system is a core module in the application and user access is managed by top-level users within each client. The limitation is that a user can only be in one role.

4.5 - Does aXcelerate support integration with ID federation and Single Sign-On systems?

As mentioned in 4.1, this can be achieved through API integration. A session can be created and a security token can be generated for a user. The token with the user ID can then be passed into a browser request to create a session in the browser.

4.6 - Does aXcelerate have an integration with Microsoft Active Directory (ADFS / LDAP)?

We currently support an ADFS solution for single sign-on (SSO) for training administrators and students. We have the ability to extend this to other Identity Providers.
Please see our help guide here:
https://axcelerate.zendesk.com/hc/en-gb/articles/360003636216-Azure-Active-Directory-SSO-Configuration

4.7 - Does aXcelerate support integration with identity access management (IAM) systems for access governance and automated user provisioning (i.e., RSA IMG)?

Not currently.

5.0 - Software development

5.1 - Does aXcelerate have monitoring and oversight during software development (i.e., onshore, offshore/outsourced work)? Describe the controls in place.

aXcelerate does not outsource any code development affecting the core components of the system. All code is developed in-house under a strict set of development standards and a culture of continuous improvement.
We have a small team of offshore developers and QA. This team is integrated with our onshore team and must adhere to the same standards and quality control with their work. Offshore staff connect to our systems securely and are limited to only the essential systems that are required to fulfil their job requirements.
To ensure confidentiality and data sovereignty requirements, data used in testing contains no client data and instead contains dummy data generated to test the application and performance.

5.2 - How often is your product upgraded? How are these communicated? Does it cause service interruption?

Fortnightly releases are communicated through release notes and are not expected to cause any service interruptions.

5.3 - Please describe the approach to patching the underlying infrastructure.

Our infrastructure servers are patched weekly to ensure a high level of security. In addition, we utilise AWS System Manager to monitor and audit systems continuously for security patches released between update schedules.

5.4 - Do you use a Software Development Lifecycle (SDLC)? If so, is it compliant with the Software Engineering Institute's Capability Maturity Model Level 3 or equivalent?

Our SDLC would be self-assessed at the highest level of maturity. We are constantly measuring, reviewing and optimising our processes and we run our software development in a standardised predictable environment. We have weekly meetings with the entire development team specifically to evolve this process.

5.5 - Please describe your approach to the creation of Development, Test/Integration/User Acceptance and Training environments to support the implementation of the product.

Where applicable, we involve a committee of participating clients in the development process of a new feature. Initially, we develop mock designs and obtain feedback. After development, internal QA is performed before involving clients in Alpha testing to achieve a minimum viable product for release. We then use system flags to release the feature in Beta Mode so the feature can be turned on or off in the system settings. Clients can opt-in to use the feature if they wish. We do a full release and market the feature to existing users when we have a quality product with supporting documentation.

6.0 - Logging

6.1 - Does aXcelerate support security logging? Describe the minimum security event details generated by the system (i.e. User ID, Type of Event, Date/ Time, Success or Failure Indication, Origin/ Destination of Event, Identity of affected data, system component or resource.).

Many but not all changes in aXcelerate are logged with a time and user. Some critical features of aXcelerate have change logs that include value changes for key fields.
Login/Session records are stored for all administrators and students who access the system.

6.2 - Does aXcelerate support integration with external log collectors / protocols (i.e. Syslog, SNMP, SIEM)?

aXcelerate data is logged to an external SIEM that keeps within the data sovereignty requirements by storing all data within the Sydney AWS data centre. The SIEM alerts key staff in the advent of any potential misuse or malicious activity.

6.3 - Can the logs generated by aXcelerate be secured to ensure the confidentiality, integrity, and availability of data (including during transmission and storage)? Describe the security of the logs, the minimum log retention period and a minimum period where logs are immediately available.

Logging of user interaction on critical data stored in aXcelerate, e.g. unit enrolment and results/completion dates, are available as live data as a feature of the application. This data can be accessed via a reporting server where the data is no more than 24 hours old.
aXcelerate also keeps some internal logs for the usage of certain features of the system such as API calls and report requests to manage responsible use of the system.
Application logs are kept indefinitely where possible, otherwise, we maintain a 6 months retention policy. In the advent that an incident needs to be investigated, we can access these logs for review.
Other services offered by aXcelerate that are not directly related to the application can often have a shorter period of logging with a period of 14 days. In these cases, it is important to notify aXcelerate of any potential misuse of hosted systems to ensure we can investigate and retrieve logs appropriately.

6.4 - Does aXcelerate support system time synchronisation to ensure log timestamps are accurate?

We use AWS NTP servers to ensure time synchronisation across the infrastructure. Logging data is always stored in UTC time to avoid synchronisation issues and other application data is controlled by a system setting that can be customised for each tenant.

6.5 - Do you regularly review audit logs?

Yes, on a daily, weekly and monthly basis.

6.6 - What monitoring and alerting mechanisms are in place? How would we get visibility of system stability performance etc? Please describe the process of communicating service interruptions.

Clients visibility through http://status.axcelerate.com.au/
Internally, aXcelerate has a large number of automated monitoring systems that alert staff via SMS and/or email when any system is at risk. These systems proactively send alerts in advance of issues occurring e.g. System Drive Volume warnings at 70% full, High system resource usage and Load balancer performance bottlenecks.

6.7 - How are application logs managed? What is the retention period and purge policy? Is customer data stored as part of the logs?

Several logs to the system have varying lifespans depending on what is required to support an internal process, for example, Logins are held for 18 months. Most logs record a user ID which can be linked back to a user's record. Generally, customer information is not logged.

6.8 - Are all changes within the product tracked at the field level? Will the system administrator be able to review the audit trail to determine who made what change and when? Does this include new entries, updates and deletes?

Some specific fields which are classified as auditable have reports to show who made a particular change. This is only for a small subset of fields relating to changes in system settings, financial records, running reports and accredited training information that affects funding, i.e. competency status, learning start and end dates.

6.9 - Please describe the opportunity our clients have to audit the environment.

Given that the system is multi-tenanted, this is restricted however we have worked with previous clients in answering questions and conducting security vulnerability testing.

6.10 - Does aXcelerate support the auditing for the database?

Access to the database is restricted to System Administrators of aXcelerate. Internally, aXcelerate carries out database health and maintenance checks regularly. aXcelerate users have access to a reporting system for data auditing purposes if necessary.

7.0 - Security

7.1 - How frequently do you conduct vulnerability/penetration testing? When was the last test performed?

aXcelerate strictly adheres to external third-party vulnerability testing on an annual basis. The testing is generally conducted between January and March each year.
Internally, we use vulnerability and malware scanners on our application servers and perform scanning once a month as part of our update procedure.

7.2 - Can you provide an outline of the current security processes you are employing to keep our data safe?

aXcelerate keeps up to date with all required security patches for our web servers and platforms, e.g. Java/Lucee and Windows/SQL Server. aXcelerate encrypts all its database

data at rest. In addition, specific confidential data such as passwords, tax file numbers etc. is persisted in an encrypted format.
Access to all aXcelerate systems is via password-controlled credentials with enforced MFA.
All new staff complete comprehensive induction which includes training on aXcelerate's Information Security policies and procedures.

7.3 - Does aXcelerate comply with information security standards such as PCI-DSS, ISO 27001 and ASIO T4?

aXcelerate is certified against ISO 27001, ISO 9001 and DESE/RFFR compliance.[12] We are audited annually by a third-party firm to ensure we maintain compliance and uphold the standards set out within these requirements.
We are committed to the continuous optimisation of our information security. Credit card information should not be stored in aXcelerate as we do not have PCI-DSS compliance. This includes fields such as free-text note type fields. All of our 3rd-party payment providers are PCI compliant and all processing and handling of credit card information should be handled by the 3rd-party.

7.4 - Does aXcelerate comply with physical security standards such as SSAE 16, SAS 70, ISO 270001 and ISO 14001?

All the data for the aXcelerate application is stored in AWS data centres in Australia. This cloud service is compliant with a comprehensive range of standards. Their level of compliance and certification leads the industry.[13]

> **More Information:**
> AWS is a secure, durable technology platform with industry-recognized certifications and audits: PCI DSS Level 1, ISO 27001, FISMA Moderate, FedRAMP, HIPAA, and SOC 1 (formerly referred to as SAS 70 and/or SSAE 16) and SOC 2 audit reports. AWS data centres have multiple layers of operational and physical security for data and networks.[14]

7.5 - Can aXcelerate be protected from untrusted networks?

OR

Does aXcelerate provide protection for its data stores and other critical components?

OR

Does aXcelerate have security features at the host level? (e.g., Endpoint Protection such as AV, IPS, Host firewall).

aXcelerate implements the AWS Security Groups feature throughout all of its live production and testing infrastructure. This acts as a firewall control to facilitate server-to-server communication within the network whilst allowing aXcelerate System Administrators the access they require. Ports are only open on these connections where required. Effective

[12] https://www.axcelerate.com.au/information-security
[13] For more information, see https://aws.amazon.com/compliance/
[14] For more info, see https://aws.amazon.com/security/

configuration of AWS Security Groups ensures that all data stores and virtual machines running aXcelerate cannot be accessed by any untrusted networks.
aXcelerate also implements a Web Application Firewall (WAF) that protects the applications and APIs against common web exploits and bots activity that could affect service availability, compromise security, or cause the misuse of excessive resources.
Where applicable, AntiVirus is configured to scan at regular intervals, with all findings logged and reported to the SIEM.

7.6 - What physical security controls are there to protect the locations storing/ processing/ transmitting customer data in electronic and/ or physical form? E.g. Data Centre, Office Premises?

Physical:
AWS provides physical data centre security for the premise where your data is stored. At the aXcelerate office premises, the building is secured by a locking system on the front door that requires a FOB key to open the door from the outside.
Electronic:
AWS security groups and IAM roles protect data at storage and in transmission. This controls access between resources within the data centre and also allows aXcelerate staff to access particular AWS resources securely whilst keeping these resources inaccessible from traffic outside our network.

7.7 - Do you retain records for physical access control/ video camera/ visitor movement?

Regarding the data centre, again AWS is responsible for this. In our office, we regard visitor movement as very low risk and do not record this activity.

7.8 - Does aXcelerate have security controls to protect against malicious code (i.e. secure code review)?

Code is reviewed through GIT source control which identifies the developer responsible for any code change. All interactions between the application and database are parameterised to prevent SQL injection. There are unit tests on all service and DAO layers in the application.

7.9 - Does aXcelerate have controls in place that would ensure changes and modifications in its components/software (custom or packaged) do not reduce aXcelerate's security profile?

The system is architected in a way that separates security from feature enhancements. Features of the software do not require any server/network configuration and new features implement the centralised user-level security mechanism.

7.10 Does aXcelerate have anti-DDoS attack defence?

Yes, AWS states that all AWS customers benefit from the automatic protections of AWS Shield Standard. AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards web applications running on AWS. aXcelerate also implements API

throttling and has extensive monitoring of the application to enable us to identify and quickly respond to any such attacks. For more info, see https://aws.amazon.com/shield/

7.11 - Does aXcelerate have Web Application Attack Defence?

aXcelerate implements an AWS-managed Web Application Firewall that scans and blocks malicious requests before they enter the network.
aXcelerate undertones yearly penetration testing to ensure that any high-level vulnerabilities such as Cross-site Scripting, Password Brute Force hacks, SQL Injection, etc. have been addressed.

7.12 - How does aXcelerate securely send Emails on the client's behalf?

aXcelerate can be configured to forward all mail through the client mail server. aXcelerate provides mail server configuration including security credentials in its system settings.

8.0 - Incidents

8.1 - Can aXcelerate support monitoring for security incidents related to data confidentiality, integrity, and/or system/data availability?

AWS CloudWatch, AWS CloudTrail, AWS GuardDuty and an enterprise SIEM are used to identify anomalous activity and attempts at accessing the infrastructure and exfiltrating data. Any information regarding system availability is communicated to the client on an Adhoc basis via our internal in-app notification system.

8.2 - Do you implement remediation strategies within a reasonable amount of time?

We have clear and practised procedures for the prevention and resolution of any incident or bug. Critical issues found in the software can be hot-fixed on the day of discovery and depending on the severity, issues are usually resolved between 1 day and 2 weeks. Our culture of continual improvement ensures that instance is investigated.

8.3 - Do you conduct investigations into security breaches and implement remediation strategies?

Should this event occur, the same principles would apply as per the previous question.

8.4 - Do you conduct regular security training for all staff to prevent inadvertent disclosures?

aXcelerate staff work in a secure environment and are given sufficient knowledge to support the data security of our customers as part of the onboarding process. This includes review and acknowledgement of appropriate security policies and procedures. Ongoing security training is a recent initiative for our staff.

8.5 - Do you immediately notify your customers of any security breaches?

Our procedure is to notify all staff and any/all affected clients immediately. No security breaches have been recorded to date (since its establishment in 2009).

8.6 - Do you notify your customers of any data corruption/loss including the nature and extent of the incident?

Yes. As soon as possible.