# OpenAthens security guide

| | |
|---|---|
| **Authored by:** | Adam Snook |
| **Creation Date:** | 20 July 2017 |
| **Last Revision Date:** | |
| **Version:** | |
| **Reviewed by:** | |
| **Approved by:** | |
| **Review Period:** | Annually |
| **Next review date:** | |
| **Unique reference:** | |

# Contents

# 1. Security

*1.1. How do you guard against and evidence intrusion into your network, and unauthorised access of your systems and data (PCI-DSS compliance, Data Protection Act, US-EU Safe Harbor, intrusion detection / prevention, 2 factor authentication, patching for security, vulnerability scanning, customer segregation, AV / malware protection)?*

As a provider of sensitive IT services, we have utilised good industry practice across our whole business operation to guard against intrusions to our networks and unauthorised access to systems and data. To ensure the confidentiality, integrity and availability of our services we have retained responsibility for all aspects of the service from networks, datacentre hosting, development and service operation and support. This enables us to provide a unique level of assurance.

Eduserv has been continuously certified against ISO27001:2005 and ISO27001:2013 for many years and applies all normative controls to protect our customers' information assets.

All data is held securely on Eduserv's own infrastructure in Eduserv's tier III data centre facilities in multiple geographical diverse locations in the U.K using a proportionate physical, technical and operational controls. Eduserv uses different firewall and intrusion detection systems from dual vendors internally and on network edge which is monitored by security operation teams 24/7. All Eduserv device firewall/security device logs are sent to our protective monitoring team for security analysis and to investigate and identify security anomalies. We have a dedicated security incident response plan steps with trigger identify security incident/response/remediate .

The OpenAthens systems and services are subject to continuous monitoring and regular security testing. We conduct our own internal penetration tests annually.

As defined under the Data Protection Act 1998, Eduserv's role is as data processor for all identity provider and service provider clients; the data controllers are the relevant OpenAthens clients. As such our primary responsibility is to process data only in accordance with client instructions.

Databases containing personal data are logically and physically segregated and are not directly accessible from outside the relevant Eduserv network. Only appropriate data is available to OpenAthens users and vetted OpenAthens administrators through the web, and these sites are protected with usernames and passwords, as well as IP address recognition for the administration website.

Our security posture is independently assessed routinely. External audits are conducted every 6 months by an ISO27001 auditor and separately by UK Government accreditors.

Eduserv employs a Chief Information Security Officer, an Information Security Manager and a Compliance Officer to oversee the security of data.

*1.2 If the solution is going to be vendor hosted, does the data center support the AT 101 SOC 2 Type II audit standard? In addition, please provide the most recent certification/audit report.*

OpenAthens is hosted within Edsuerv's UK based data centres which are continuously certified against ISO 9001 and ISO 27001.

# 2. SLA

*2.1. What are your SLA's (availability and performance globally, recovery time and point objectives), how are they calculated and measured and reported to us?*

## Service incidents

| Severity Level | Description | Response time | Resolution Period |
|---|---|---|---|
| **Severity Level 1** | An incident that results in a complete failure of the OpenAthens service affecting all users at one or more sites or regions. | 1 Hour | Incidents to remedied within 4 hours |
| **Severity Level 2** | An incident that results in a failure of the OpenAthens service resulting in the unavailability of one or more key functions of the OpenAthens service to users. | 2 Hours | Incidents to be remedied within 8 hours |
| **Severity Level 3** | An incident that results in a partial failure of the OpenAthens service resulting in the unavailability of part of one or more key functions of the OpenAthens service to users. | 4 Hours | Incidents to be remedied within 24 hours |
| **Severity Level 4** | An incident that results in a partial failure of the OpenAthens service resulting in minor usability or cosmetic issues with part of one or more functions of the OpenAthens service for users. | 24 Hours | Incidents to be remedied within 10 days |

Notification of incidents will be provided by the OpenAthens Service Desk during working hours to customers via the OpenAthens status page at http://status.openathens.net.

## Service Levels and Performance Indicators

a) Eduserv shall provide a service that is available 99.95% of the time, other than when caused by factors outside Eduserv's control (Force Majeure) and service affecting maintenance
b) Authentication assertions responded to within 3 seconds 99.99% of the time, sample on a 60 second basis measured locally through random sampling of each Authentication Point
c) Service Affecting Maintenance of the Single Sign-On and MyAthens services is not to exceed 25% of the total 'At Risk' hours for a calendar quarter;
d) Additions and updates to OpenAthens account data will be reflected in the single sign on service and MyAthens within 15 minutes.

*2.2. Are there any specific events (scheduled maintenance) that do not contribute towards the SLA's?*

Service affecting maintenance is defined as planned maintenance which causes the service to be unavailable to any licenced organisation. As far as possible, planned maintenance activities shall be synchronized and shall fall during the "at risk" period from 07:00-09:00 (UK time) on Tuesdays, Wednesdays or Thursdays. Notice shall be given on the OpenAthens Status page no less than two working days prior to the maintenance work.
We operate a high-availability service so all services are scheduled to be available 365 days a year and 24 hours a day, apart from planned maintenance times but there is no regularly scheduled downtime for any service.

*2.3. What is the escalation process for issues identified by us and expected response times?*

Service support is provided through our ITIL accredited OpenAthens Service Desk during UK working days (Monday to Friday from 09:00-17:30), dealing with enquiries from OpenAthens administrators at licenced organisations, by telephone, email and via our web portal. Refer to section 2.1 for information regarding response times.

Organisations purchasing OpenAthens through one of OpenAthens' partners will be directly supported by the partner so should also consult them for their processes.

*2.4. What is your process for resolving SLA breaches (regular reviews and time frames for remedies)?*

SLA breaches are reviewed to identify underlying causes so items can be added to our software development/infrastructure backlog and prioritised accordingly. Account managers will follow up with customers where appropriate.

# 3. Continuity and Backup

*3.1. What techniques, whether through software, hardware, processes (testing of) or 3rd party agreements, guarantee your service availability and restore it when degraded (business continuity process including testing and continuous improvement, fault tolerant architecture)?*

## Availability

The OpenAthens service is a HA (High Availability) service operating from multiple data centres (DC), of which the service can run from any. Incremental backups are taken every hour and full backups are taken every night. We also synchronise data in real time between datacentres to multiple machines within those DCs. Should data recovery be required it will be restored to 100%. The retention period for backups is 7 days.
The infrastructure design ensures:

- The service is hosted and located at multiple geographically separate datacentres with failover options when one data centre becomes unavailable.
- Each server/service has at least one 'disaster recovery' server. This ensures that if there is a hardware failure then the service can continue.
- Real-time data replication ensures that database storage is fully resilient.
- Any data centre we use must meet high standards with regard to two independent sources of power, fire and flood detection, fire suppression and redundant cooling.
- We have diverse network links from multiple suppliers into our datacentres.

The OpenAthens service operates a number of secure authentication points (AP) in order to provide a high-availability, resilient access management service. These are made available to any supported service provider with a single URL that automatically redirects users to an available AP. Every AP has a simple, intuitive interface and is configured with the standard error handling process.

The operational service is monitored 24x7x365 using monitoring tools to provide information on availability, response times and hardware utilisation with alerts being sent to the Service Desk in the event of thresholds or issues being detected or to an on-call team out of hours. System logs are reviewed regularly to ensure performance remains within acceptable operational levels, with a view to adding additional server capacity if required.

Some of these checks include:

- Automated logins to each Authentication Point to ensure each authentication server is available
- Sample authentication times are taken from each authentication server to ensure requests are being processed within reasonable timescales
- Database replication latency is monitored to ensure OpenAthens applications are using up-to-date data when processing requests
- Fast access data that is shared between the OpenAthens servers is monitored to ensure each server is using the latest version
- The load on each server is monitored to ensure requests are being distributed evenly

This continual monitoring, both automatic and manual, enables us to provide a high availability service to all OpenAthens customers, and Eduserv's business continuity plan is subject to annual review.

## Testing

- Unit/component testing is carried out by the developers to ensure the components operate as specified in the requirements and in the system design documents.
- System integration testing is carried out by the QA team. This includes cross browser testing of new functionality and regression testing to ensure that the system has not been adversely affected by changes. This will include testing interaction with individual Service Providers systems, where appropriate. Performance testing, accessibility testing and independent penetration testing is also included.

For each release of the OpenAthens service, the following deliverables are produced by the test team.

- Test approach - a document describing the scope, approach, resources and schedules of intended testing activities. It identifies test items, the features to be tested, the testing tasks, who will do each task, and any risks requiring contingency planning
- Functional test scripts - test cases to detail how each functional requirement should be tested. (This includes test design, test case specifications and test procedure specification)
- Test results document(s) - These will be updated as each test is executed. They will include a copy of the test script with a record of when the test was run and whether the test passed or failed.
- Test summary report - A summary of testing completed.
- Release notes - details of new features, bugs which have been fixed and known issues.

*3.2. Specifically, how do you ensure data is not lost, whether through logical and physical failure, the latter ranging from single component failure to a disaster scenario?*

- At every level from the server all the way out to the internet every piece of hardware or cable has an independent backup. Servers have multiple independent network ports. Switches, routers and firewalls all are able to failover to backup devices. Multiple independent ISPs connect to the data centres.
- One of our data centres is classed as the primary with most services hosted there, with their backup servers at the disaster recovery data centre. This is with the exception of the single sign-on (SSO) service which has live servers hosted in both data centres. Constant monitoring of the SSO service ensures that if the SSO servers become unavailable at one

data centre then the other one will take on the full load of the service, automatically removing the inaccessible servers from service.

# 4. Capacity Planning

*4.1. How do you capacity manage your systems and organisation to meet growing demand (headroom, peak loads, priority customers, stepped costs) from one or many customers without impacting availability, performance or service?*

- We routinely monitor load and usage on the OpenAthens infrastructure.
- Performance monitoring information and growth projections are fed into quarterly capacity planning meetings to enable advanced planning of any increase in capacity.
- Our infrastructure currently has significant spare capacity.

# 5. Delivery and Integration

*5.1. How do you assure quality in your delivery process to minimise impact to the customer (API versioning, software upgrades and support life-cycle)?*

Eduserv is certified to ISO 27001. Our approach to quality assurance is based on the ISO9001 standard, which draws upon aspects of industry specific standards, such as ISO27001 Security, and ISO20000 Service Management.

Eduserv has adopted a process approach to quality management. This first requires that processes are in place that are sufficient to meet customer, statutory and regulatory requirements and that these processes are recorded and followed by all staff. The processes, and the services they produce, are then monitored and reported on at regular intervals to ensure their quality. In addition, methods of capturing and actioning ideas for improvements to processes are put in place to ensure continuous improvement.

The Eduserv IMS houses all of Eduserv's process descriptions, both for record and to ensure easy reference by any member of staff. These descriptions cover all areas of the organisation, down to the level of individual roles, and map inputs, processes, outputs and related records. Individuals are expected to follow these processes and teams are expected to maintain mechanisms for capturing, recording and actioning feedback. In this way, on-going quality is ensured and continuous improvement encouraged.

A documented testing process is followed for all releases of new OpenAthens Products. This process covers unit, system and integration testing performed on a dedicated testing environment to establish a release as meeting agreed completion criteria and being functionally ready. Releases are then migrated to a separate staging environment for non-functional testing which covers security, stress and performance tests.

Once tests are passed and a candidate release is ready for production it is passed to a managed release process. A change control is raised detailing plans for rolling the change out, risks, impacts and plans for rolling back. Major releases require a meeting of a change advisory board (cab). All changes require authorisation from the OpenAthens Testing Team, Service Desk and Management. All releases of OpenAthens are version controlled and release notes are included to communicate changes included in the release. Releases for SP & LA made available from a download page in OpenAthens.net, together with installation instructions. At least one prior release of the product will continue to be available to customers.

Customer communication of an impending release is managed through a customer service status page. 5 working days' notice is given for major releases and 2 working days' notice for small releases. Where a release has impacts on customers beyond installing a new version this is communicated by e-mail to a customer mailing list.

Any faults identified with a release are reported to the OpenAthens Service Desk in the first instance and then triaged based on impact and severity then fed into the development schedule for inclusion in a future release.

Customer satisfaction with the quality of our products is monitored via a variety of channels. We review OpenAthens support desk calls to identify common customer issues, ideas and requests and have a feedback mechanism built into the helpdesk system itself that allows customers to provide feedback when updating their support calls. We have dedicated customer relationship managers who provide points of contact for OpenAthens customers and we also maintain a regular Development Advisory Group made up of representatives from the community of OpenAthens users.

All the feedback we receive is used to further inform our internal processes and procedures as well as the development roadmap for the product itself and ensure we continue to deliver a quality product and service which meets the needs of our customers.

*5.2. How do you integrate pre-production services for development and testing?*

The development process is based on the SCRUM agile process. This involves teams of testers and engineers working together in time boxed development sprints (two weeks) to a deliver a predefined sprint goal. During a development sprint, regular releases are deployed to a test environment for testing. This level of integration between development and testing processes provides rapid feedback and correction of faults.

A continuous build environment is used to build applications and run unit tests and automated tests. Code measurement tools are used to monitor and report code quality and test coverage

# 6. Staff procedures, policies and privacy

*6.1. Is there a documented privacy policy or procedures to protect confidential information provided to service provider by client?*

Eduserv has a company policy and employees give undertakings within their employment contracts. In addition, our 27001 certifications require a rigorous approach to confidentiality with annual training for all staff.

*6.2. Are there documented policies, procedures, and controls to limit access based on need to know or minimum necessary for its employees, agents, contractors (or others as applicable)?*

Technical security controls are in place to limit access to assets and data based on individual roles and responsibilities i.e. Access is only given to those that require it.

*6.3. Are staff technically prevented from accessing the cloud environment via non-managed private devices?*

Staff are subject to an acceptable use policy (AUP) that stipulates from what devices they may access the environment and in what circumstances.