Security of Learnosity APIs

An overview

Learnosity has a policy of continuous improvement. Information herein is provided in good faith and is accurate at the time of writing. However, based on knowledge and experience, Learnosity may update its security at any time. Please send any suggestions to improve this document to: info@learnosity.com.

Learnosity

Overview

Learnosity (www.learnosity.com) is a Dublin-based education technology company specializing in digital assessment solutions. We provide a comprehensive suite of APIs and tools that enable clients to build, deliver, and analyze assessments at scale. Our solutions serve a diverse range of sectors, including K–12 and higher education, corporate training, government, and professional certification.

We maintain an active ISO 27001-certified Information Security Management System (ISMS) supported by dedicated Security and Legal teams. The ISMS is based on mitigating risk, the Kaizen philosophy of continuous improvement and a strong commitment to industry-recognized security standards. We have consistently achieved an exceptionally high level of uptime for our cloud solutions, around 99.98% over several years.

Our APIs products are hosted on Amazon Web Services (AWS) infrastructure, with servers located in Oregon, Virginia, California, Sydney and Ireland. The delivery platform includes multiple layers of protection, including physical safeguards and environment controls within AWS data centers, granular access management, redundant power suppliers, geographically replicated backups, and comprehensive disaster recovery processes to ensure service continuity across regions.

This white paper provides an overview of the security of Learnosity's core API software products, including Learnosity Author, Learnosity Questions, Learnosity Math, Learnosity Assessments, and Learnosity Analytics. It outlines the technical, procedural, and operational measures designed to maintain the confidentiality, integrity, and availability of customer data.

Some of the key capabilities include:

- High availability and resilient service.
- Employee vetting and ongoing data security and privacy training.
- Strong physical and environment protections at AWS data centers.
- Geographically replicated backups.
- Uninterruptible power supplies with multiple connections to the grid through various substations.
- Emergency generators with on-site fuel reserves for extended outages and planned maintenance.
- Disaster Recovery processes to maintain service continuity, including the possibility to quickly build and restart the service from another AWS region.

Third Party Certifications and Accreditations

ISO 27001

Learnosity is ISO 27001:2022 certified. The scope of certification covers the personnel, systems and facilities supporting our APIs activities.

This includes the activities of our employees, externally hosted information processing services/ systems and the management of third parties providing support services to Learnosity business and our customers, in accordance with the ISO 27001 Statement of Applicability.

A copy of our ISO 27001 certificate is available on the Learnosity website at https://learnosity.com/platform/security/, or by request to our Security Team. Our formal Statement of Applicability is available upon request; however, all ISO 27001 controls are applicable.

Cloud Security Alliance (CSA) Security, Trust, and Assurance Registry (STAR) Registry

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to promote the use of best practices for supplying security assurance within Cloud Computing.

CSA's Security, Trust, and Assurance Registry (STAR) is an industry leading program for supplying assurance and validation that a participant is following security best practices for cloud providers. By completing the CSA STAR self-assessment, Learnosity shows transparency via a public report of the security measures in place to protect our customers' data.

You can review our self-assessment at:

STAR Registry Listing for Learnosity | CSA.

EU-U.S. Data Privacy Framework (EU-U.S. DPF)

The EU-U.S. Data Privacy Framework (EU- U.S. DPF) is an international framework established between the European Union and the United States to enable lawful and secure transfers of personal data.

It ensures that organizations receiving EU personal data in the U.S. provide protections equivalent to those required under the EU data protection law.

Learnosity is certified under the EU-U.S. Data Privacy Framework (EU-U.S. DPF), including the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF).

Data Centers

AWS offers a robust and secure infrastructure that meets a wide range of international compliance standards. At the time of writing, AWS holds multiple global certifications for cloud security, availability, and compliance. For more details on AWS security practices, please see: https://aws.amazon.com/security/.

Physical Security Measures

AWS maintains highly secure data centers around the world, employing a multi-layered approach to protect customer data. The following measures are implemented to safeguard physical infrastructure:

- **Access Authorization and Monitoring**
  Physical access to AWS data centers is strictly controlled. All access requests must be pre-approved and include business justification. Visitors are granted access based only on operational necessity and for a limited time. Every access attempt is logged and monitored.
- **Perimeter Security**
  Data center perimeters are secured by reinforced fencing, surveillance systems, and security patrols. Physical barriers are made from steel and concrete, and are monitored 24/7 by dedicated security teams using CCTV and motion-detection systems.
- **On-Site Security Staff**
  Professional security officers are stationed at all facilities. They perform routine patrols, monitor entrances and exits, and respond to physical security alerts in real time.
- **Entry Controls**
  Access to AWS data centers requires multi-factor authentication (MFA), including biometric verification. Identity checks and access rights are enforced before individuals are allowed entry into specific areas of the facility.
- **Data Center Floor Controls**
  Once inside, access to the actual data center floor is further restricted. Individuals must pass through full-body metal detectors, and only approved equipment and devices are permitted.

AWS data centers are designed to ensure maximum uptime, resiliency, and security:

- **Power Continuity**
  Uninterruptible Power Supplies (UPS) provide immediate backup power during short-term outages, as well as on-site diesel generators.
- **High-Speed Connectivity**
  AWS connects its data centers via a global network of high-speed fiber links, ensuring low latency and high availability between Regions and Availability Zones (AZs).
- **Redundant Network Architecture**
  AWS uses a fully redundant N+1 design for power, networking, and connectivity infrastructure, ensuring no single point of failure.

- **Data Security and Encryption**
  All customer data is encrypted using AES-256. AWS supports TLS 1.2 or higher for data in transit.
- **Data Replication and Regional Resilience**
  Customer data is replicated across multiple AZs within a Region. AWS also supports cross-region replication and multi-region failovers.
- **High Availability Architecture**
  AWS AZs are designed to be independent from one another and are physically separated within a geographic region. This helps ensure high fault tolerance and availability.

Network Security and Connections

Network Security

A summary of the security provided by the network infrastructure:

- All inbound and outbound internet traffic to AWS-hosted services is encrypted using TLS ensuring secure data transmission.
- The application load balancers are protected by AWS WAF which is deployed across multiple Availability Zones for redundancy.
- Each EC2 instance and service tier is secured with Security Groups and Network ACLs.
- Bastion Hosts are used for secure administrative access to instances in private subnets, enabling controlled and audited SSH access without compromising system integrity.
- Instances use Amazon Inspector or third-party tools for antivirus protection.

For a current report on the SSL/TLS configuration and certificates used by Learnosity APIs, see:

- SSL Server Test: annotations.learnosity.com (Powered by Qualys SSL Labs)
- SSL Server Test: assess.learnosity.com (Powered by Qualys SSL Labs)
- SSL Server Test: authorapi.learnosity.com (Powered by Qualys SSL Labs)
- SSL Server Test: author.learnosity.com (Powered by Qualys SSL Labs)
- SSL Server Test: central.learnosity.com (Powered by Qualys SSL Labs)
- SSL Server Test: console.learnosity.com (Powered by Qualys SSL Labs)
- SSL Server Test: data.learnosity.com (Powered by Qualys SSL Labs)
- SSL Server Test: eventbus.learnosity.com (Powered by Qualys SSL Labs)
- SSL Server Test: events.learnosity.com (Powered by Qualys SSL Labs)
- SSL Server Test: feedbackaide.learnosity.com (Powered by Qualys SSL Labs)
- SSL Server Test: items.learnosity.com (Powered by Qualys SSL Labs)
- SSL Server Test: learnosity.com (Powered by Qualys SSL Labs)
- SSL Server Test: ptea.learnosity.com (Powered by Qualys SSL Labs)
- SSL Server Test: questions.learnosity.com (Powered by Qualys SSL Labs)
- SSL Server Test: reference.learnosity.com (Powered by Qualys SSL Labs)
- SSL Server Test: reports.learnosity.com (Powered by Qualys SSL Labs)
- SSL Server Test: schemas.learnosity.com (Powered by Qualys SSL Labs)

System Connections

Secure End-User Access
Participants, candidates, and administrators connect to the AWS-hosted service using TLS 1.2 or 1.3 with 128- or 256-bit encryption via their web browsers. Connections enter the system through the AWS Network Load Balancer (NLB) or Application Load Balancer (ALB), both fronted by AWS WAF for web traffic filtering.

All subsequent communication flows through the AWS Application Load Balancer, which securely routes traffic to backend services within Amazon VPC.

Administrator Access for Platform Maintenance
Platform administrators securely access the AWS Production environment using RDP over a VPN connection. Access is routed through a hardened EC2-based Bastion Host in a public subnet, which acts as the single controlled entry point to reach private instances.

VPN connectivity may be established using AWS Client VPN, AWS Site-to-Site VPN, or AWS Direct Connect (if on-premises integration is required).

Learnosity APIs Infrastructure

Learnosity is designed as a Service Oriented Architecture (SOA) which means that each API provides a service which may be used directly or combined with other services to provide higher level services for other systems. It has been designed with a simple and robust setup that allows scalability at all layers of the system and ensures that each layer can have additional capacity added as appropriate.

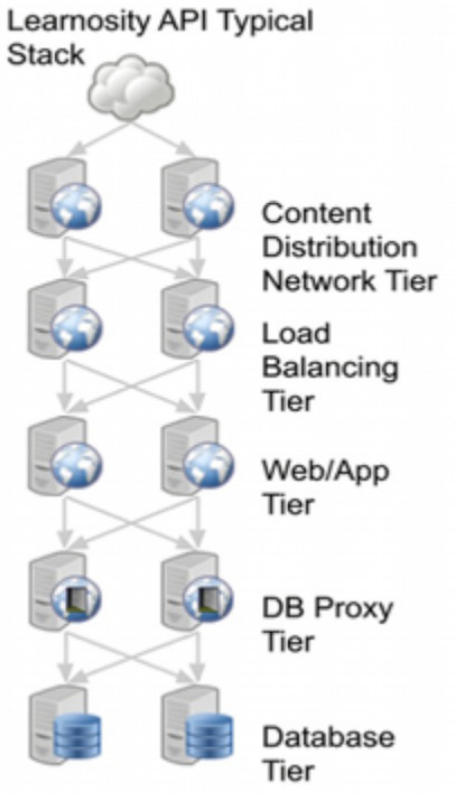
System Tiers

Content Distribution Network
We use AWS CloudFront to deliver content in a quick and reliable manner.

Load Balancer Tier
Our load balancing system automatically distributes user traffic across multiple servers and regions.This setup keeps performance consistent and ensures uninterrupted service.

Web/App Tier
The web and application layers are designed for efficient results. Each server can handle any user request, allowing us to scale up or down instantly based on demand. This prompts fast response times and reliable performance

DB Proxy
Database management layer is used to handle communication between the application and the databases. This ensures that we can control the number of database connections and provide redundancy and scalability.



Database Layer
Data persistence is handled by a fleet of PostgreSQL databases that are sharded by clients and by pseudonymous user id. This design allows each DB to be standalone as it is not required to communicate with other databases in the system which greatly simplifies configuration, improves performance and ensures flexibility.

Back-end infrastructure

Deployment and Tenancy
Learnosity APIs are multi-tenant at the application layer but can be single or multi-tenant at the database layer. On a given multi-tenant database server in a particular region, we use individual user grants per application with secure password and application Access Control Lists (ACLs). We audit and monitor all activity by centralized logging; monitoring for anomalies and raising alerts on any suspicious activity.

Technology Components
We utilize the following core components in our infrastructure:

- Centos Linux running on EC2.
- Nginx for front end web servers.
- PHP-FPM and Go for application servers.
- MariaDB and PostgreSQL for database layers.
- Memcache and Redis for caching of non-persistent data.

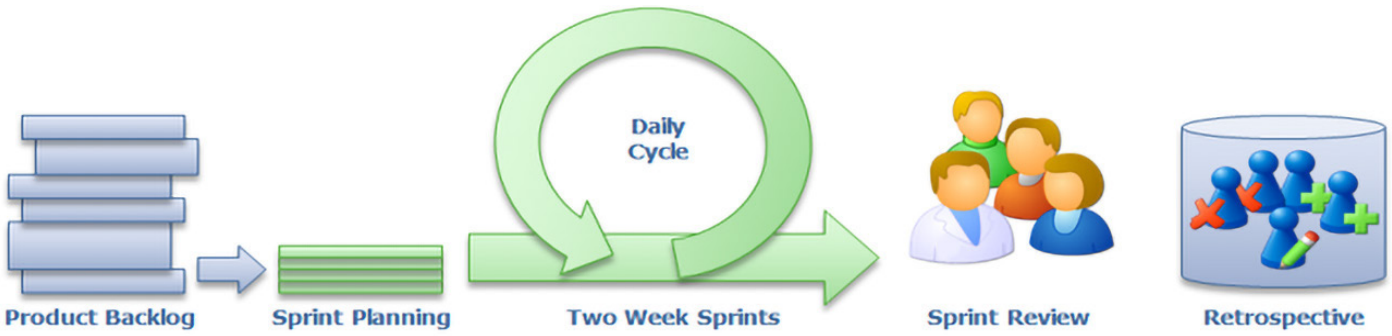
AWS Components
We leverage the following core AWS components to provide a scalable infrastructure:

- EC2 (Elastic Cloud Compute) - used for all machines running in production environments.
- ELB (Elastic Load Balancer) - used to distribute load among machines in the API Clusters.
- SQS (Simple Queue Service) - used for asynchronous message queueing.
- RDS (Relational Database Service) - used for database persistence.
- S3 (Simple Storage Service) - persistence of files for audio, images and any other media and data lake storage.
- Redshift - used for data warehousing.
- CloudFront CDN - Content delivery network with edge locations globally.

We currently utilize the following AWS regions: Virginia, North California, Oregon, Sydney, Ireland.

Application Development and Security Monitoring

Learnosity uses the Secure Development Lifecycle for Agile:



Learnosity developers also use the SCRUM/Agile software development methodology:

- The team works in three-week sprints, with tasks prioritized and assigned by the Product Owner.
- Each team is responsible for testing their own work using automated checks, integration tests, exploratory testing, and security testing.
- After local testing, changes are deployed to a staging environment through the release process. Developers confirm deployment success, review automated test results, and perform targeted testing to verify the functionality of the changes.
- At the end of each sprint, integration testing is carried out during a defined staging window, when engineers test changes across edge cases and dependent areas. Once testing has passed, codebases are tagged for release.
- After all changes are tested and verified, the release is deployed to a QA environment that mirrors production. Teams validate that environment-level configurations work correctly.
- Once all teams confirm readiness, approval is given to deploy the code into production, with post-release monitoring and checks in place.

All developers are trained and coached to ensure coding follows best practice. This ensures the developers:

- Are up to date with the latest techniques.
- Understand how to mitigate known issues.
- Provide feedback to others about new/additional issues they have found.

The development teams follow Agile SDL best practices with regards to building functionality and features. Common threats are mitigated through secure coding practices based on the work of the Open Web Application Security Project (http://www.owasp.org/).

Testing is embedded within each team's development process and follows industry best practices to deliver thoroughly tested applications at the end of each sprint. Learnosity believes in quality from the outset and because of this we use automated:

- Regression testing
- Build and deployment testing
- UI Testing
- Service-Level testing
- Unit tests

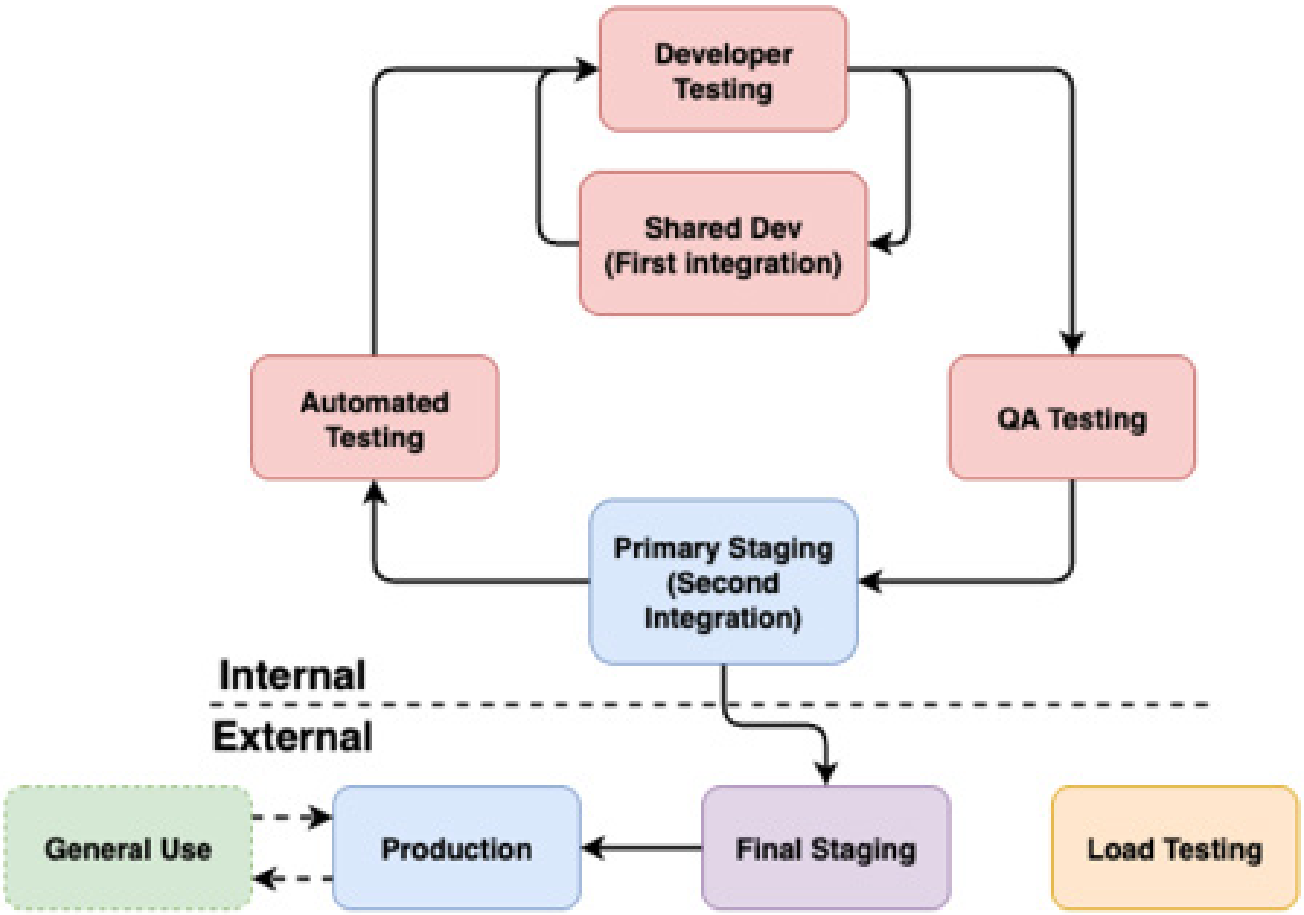
Performance of the Delivery Platform
Learnosity's aim when testing APIs system performance is to always exceed expected customer load, so as to always be ready to meet the requirements of our customers.

Our world class customer support team consistently works with customers to offer solutions and advice for them to achieve the highest performance for their usage and provides an ongoing feedback loop to Learnosity resource teams to discover additional improvements.

Learnosity APIs internal performance testing focuses on scalability and stability by structuring application infrastructure to be best fit for known customer usage patterns. The routine load of the system sees Learnosity APIs consistently handling half a billion requests daily.

Learnosity uses locust for automated load testing and stress testing of APIs. The performance benchmark is strategically set well above expected customer load for each school year.

The performance testing is conducted by simulating excessive load against a production region dedicated to load testing.



Performance Monitoring
The Learnosity APIs system is constantly monitored by globally positioned resources for performance and scale. We use Datadog for internal application and system monitoring, while the status page is used to provide service status to customers.

https://status.learnosity.com/

Data Security Policy

Learnosity has a comprehensive Data Security Policy in place that applies to all employees and authorized contractors.

A summary of the policy:

- Background checks are carried out on all new employees and authorized contractors.
- They are required to:
  - Sign a confidentiality agreement
  - Commit to Learnosity's Data Security Policy
  - Sign Rules of Behavior
- Data Security and Privacy training is given to each new employee and authorized contractor.
- Data security and information security awareness briefings are given to all employees and authorized contractors regularly.
- Our Information Security Officer is responsible for compliance and recording security incidents if they occur.
- A password policy requiring strong passwords and use of MFA on company devices where available.
- All employees and authorized contractors must pass annual tests on Learnosity's Data Security Policy.
- As employees and authorized contractors leave, procedures to remove access (including physical) to company data and equipment are carried out.

Accessing stored data

- A limited number of employees in technical support and related areas can request access to customer areas to assist customers with modifying their installation of the application or troubleshooting issues. Any such accesses are logged and monitored.
- Learnosity keeps customer data strictly confidential and does not share it with any unauthorized third parties, nor use it for its own marketing purposes.
- Unless required by law, Learnosity will not release customer data to government bodies. If a request is placed by a government body for access to customer data, we will only provide the data if our Legal Counsel advises that it is mandatory to do so. Unless prohibited by law, Learnosity will consult or inform the customer prior to releasing data based on a government request.

Service Continuity

Learnosity has a history of providing reliable APIs solutions and takes business and service continuity seriously. We know the importance to our customers and stakeholders of robust assessment technology. Therefore, we have carefully planned our service continuity measures to ensure a reliable service for customers. We have prepared for foreseeable disruptions by putting in place a system of roles and responsibilities so we can evaluate and resolve unforeseen disruptions and ensure that we maintain and quickly restore the service. For up-to-date details about the uptime, please refer to: Learnosity Status.

Our employees are motivated, well-trained, and highly experienced, and Learnosity is committed to our customers' long-term success. We have put in place professional measures for service continuity. In case of any disaster or disruption, we will use the strongest efforts possible to get our service working again reliably and robustly.

Amazon Web Services (AWS)
Learnosity chose to host its APIs SaaS services in Amazon Web Services (AWS) data centers for some of the following reasons:

- AWS offers an impressive 99.99% uptime SLA for key services across its global cloud infrastructure, including multiple Availability Zones (AZs) in each region for fault tolerance.
- Amazon, along with global enterprises such as Netflix and NASA, runs mission-critical workloads on AWS, demonstrating AWS's confidence in its own reliability.
- AWS provides fully managed services such as Amazon RDS for SQL Server, Amazon Aurora, and Elastic Load Balancing (ELB). These services handle maintenance, patching, and scaling with minimal downtime and automated failover for high availability.
- AWS offers cross-region replication and backup services for robust disaster recovery planning. It provides strong encryption standards (AES-256, TLS 1.2+), extensive security monitoring via AWS CloudTrail, Amazon Guard Duty, AWS Security Hub, and CloudWatch Logs for real-time analytics.
- The AWS global network is architected with full N+1 redundancy to maintain availability even in case of component failures.
- AWS uses AZs within regions to physically separate components, significantly reducing the chance of a single outage affecting multiple instances.
- AWS data centers are equipped with emergency backup generators with on-site fuel reserves for sustained operations during extended outages and scheduled maintenance.
- UPS provides protection against short-term outages, helping to ensure continuous service delivery.

Routine Maintenance

Routine maintenance is performed during low-traffic periods while the system remains fully operational to avoid service disruption.

During these periods, individual servers or services in the cluster may be taken in and out of rotation, which can occasionally cause minor reductions in performance.

Customers are notified of scheduled routine maintenance through our status page and email notifications, giving them advance notice of any potential impacts.

Scheduled Downtime Maintenance
Thanks to AWS's redundancy and multi-AZ architecture, most updates and maintenance can be completed without any downtime.

Planned Downtime will be kept to an absolute minimum and is expected to total no longer than seven hours in any given quarter. Exceptions to this will be mutually agreed in advance.

Learnosity must give at least five business days' notice of when Planned Downtime is going to occur. All Planned Downtime needs to be approved by the customer.

Emergency Maintenance
In unforeseen cases where Learnosity becomes aware of a serious event requiring immediate action, an emergency maintenance session may be scheduled. We will provide notice as soon as we become aware of the need for such a window.

Downtime
Because of the platform's redundancy features and failover capacities, most updates can be made without downtime.

Any unplanned downtime is recorded and analyzed to understand why it occurred and if mitigation steps can be taken to limit the disruption. We will follow through with risk management planning to ensure that this type of unplanned downtime will not happen again.

To deal with the unlikely event of a service disruption, a Disaster Recovery Plan is in place.

Disaster Recovery (DR)

To mitigate the risk of service disruptions, Learnosity has a robust Disaster Recovery Plan (DRP) in place, leveraging AWS's industry-leading infrastructure and best practices:

- Data Backups
    - Amazon Relational Database Service provides automated backups with daily snapshots and transaction logs captured every 5 minutes.

  - These backups are replicated across multiple Availability Zones (multi-AZs) and can be configured for cross-region replication to protect against regional failures.
  - The Recovery Point Objective (RPO) target is typically under 1 hour, meaning in the event of disaster recovery, it is unlikely more than an hour's worth of data would be lost.
  - The Learnosity Platform team is alerted immediately of any backup issues via automated notification systems (e.g., Amazon SNS) and can escalate to AWS Support as needed.

- Geographically Redundant Communication

  Learnosity maintains several geographically dispersed systems independent of the production environment to maintain communications during service disruptions. These include:

  - Email and CRM systems
  - Social Media (e.g., Twitter/X): Learnosity (@learnosity) / X
  - Public Status Page: Learnosity Status

  Additionally, Learnosity's staff can use third-party collaboration platforms (e.g., Slack, mobile phones, instant messenger, internal twitter feeds) to coordinate internally and maintain external communication.

  In the event of a major service disruption, staff will assess the most effective communication method and provide customers with regular updates on estimated recovery timelines.

Incident Response Procedures

An issue severity rating system determines how incidents are treated:

Item Description	Response Acknowledgement Target	Resolution Target
Urgent Issue	3 hours	8 hours
High Severity Issue	36 hours	1.5 business days*
Medium Severity Issue	1 business day*	2 business days*
Low Severity Issue	1 business day*	3 business days*

Alert Systems

Learnosity has in place three alert systems for APIs services:

1. Worldwide Monitoring

Information from these monitoring stations is available at: http://status.learnosity.com/
Learnosity monitors servers and both internal and external services that play a part in the delivery of assessments and reports, the ability to author content, the processing and availability of responses and scores, data replication, virus scanning, self-service platforms, and more, via a combination of automated alerts and active monitoring by team members.
Learnosity CloudOps and Product teams also monitor and audit backend and frontend logs. Scheduled automated internal tests around the clock further alert appropriate teams to the loss or degradation of APIs functionality.

2. User reports

The Learnosity Technical Support team typically receives user reports via a Learnosity Support portal ticket.

3. Learnosity CERT

Learnosity has a Computer Emergency Response Team (CERT) for the APIs service that monitors and provides alerts related to security vulnerabilities reports from any source.

Customer Service and Notifications

Our goal is to provide a first-class customer experience.

We provide extensive online documentation, including quick-start guides, manuals, white papers, best practice guides and communications from our customer success teams. Commercial and "how-to" information is provided by our Customer Success Teams and more detailed technical information is provided by Technical Support.

Prospective customers may call during working hours or email at any time to: support@learnosity.com. Questions are usually answered the same day.

The following support services are available:

SUPPORT LEVEL DEFINITIONS

The customer will provide 1st and 2nd Line Support, while Learnosity will provide 3rd Line Support, as defined below.

1st Line Support	The Customer's Users shall direct any initial and primary inquiries, requests and support issues with respect to the Software to the Customer's support representative or the relevant Customer's help desk.
2nd Line Support	Any queries with respect to the Software that cannot be resolved by the 1st Line Support team will be assigned to the Customer's 2nd Line Support team. An Incident which cannot be resolved by the 2nd Line Support team is eligible for escalation to Learnosity as part of 3rd Line Support.
3rd Line Support	Any Incident that cannot be resolved by the Customer's 1st or 2nd Line Support team may be escalated to Learnosity's tech support team. Only Incidents resulting from Software system or platform matters, or those that meet the escalation process defined above, shall fall under the SLA's commitments stated in the "Incident Response Procedures" section above. It is the Customer's responsibility to provide details of Incidents in the form of screenshots, logins, etc. along with any steps taken to resolve prior to escalation. Learnosity will then attempt to replicate issues in order to adequately resolve the Incident. The customer shall make available to Learnosity any team members knowledgeable about the escalated Incident. All Incidents eligible for 3rd Line Support logged with the Learnosity will be given an appropriate priority and receive a unique reference number via an online ticketing system. Ticket status and any associated updates will be accessible to the originator.

Incident Response Procedures

An issue severity rating system determines how incidents are treated:

Alert Systems

Learnosity has in place three alert systems for APIs services:

1. **Worldwide Monitoring**
   Information from these monitoring stations is available at: http://status.learnosity.com/
   Learnosity monitors servers and both internal and external services that play a part in the delivery of assessments and reports, the ability to author content, the processing and availability of responses and scores, data replication, virus scanning, self-service platforms, and more, via a combination of automated alerts and active monitoring by team members.
   Learnosity CloudOps and Product teams also monitor and audit backend and frontend logs. Scheduled automated internal tests around the clock further alert appropriate teams to the loss or degradation of APIs functionality.

2. **User reports**
   The Learnosity Technical Support team typically receives user reports via a Learnosity Support portal ticket.

3. **Learnosity CERT**
   Learnosity has a Computer Emergency Response Team (CERT) for the APIs service that monitors and provides alerts related to security vulnerabilities reports from any source.

About Learnosity

Learnosity is the global leader in AI-optimized assessment solutions.

Serving over 750 customers and more than 40 million learners, our mission is to advance education and learning worldwide with best-in-class technology.

More at learnosity.com

Learnosity