Atomic Learning Privacy & Data Security FAQs

1. What data does Atomic Learning collect?

To support the professional development, course integration, support and other educational needs of our customers, Atomic Learning may collect the following information: first name, last name, e-mail address, student ID number, role as teacher or student, institution name, building name, assessment title and scores, and learning objects viewed, grade level, area of study or instruction. Atomic Learning may also use persistent and session cookies.

The minimum student data needed to support the most basic use of the product is username and role as student or teacher. If no additional information is collected and stored, the ability to provide notifications, reports by name or location, customization of information, assessment data and other information and functionality may be limited.

2. Where and how is data stored?

Website databases, servers and equipment are contained in locked equipment racks. The equipment racks are housed in keycard accessible SAS compliant cages. The cages are located in keycard/bio-scan accessible data centers, all serviced by a SAS compliant collocation provider. Additional data center security measures include: surveillance cameras, badge IDs and limited facilities access granted to three trusted Atomic Learning employees and the SAS compliant collocation provider technicians. Network and server firewalls are configured to protect all website servers. Intrusion detection systems alert for potential malicious network activity. Website servers and equipment require administrator authentication to gain console access at all times. Limited remote management is allowed through strict firewall IP access lists and allowed to only five trusted Atomic Learning employees. Full website server privileges are allowed to only three trusted Atomic Learning employees. All data is stored in the United States.

3. Is all or some data at-rest encrypted?

Password data is encrypted.

4. How will the data be stored (cloud or local)?

Data is stored locally.

5. How is data and access separated by client? Who has access to stored information?

Each client is assigned a unique account ID that is used to separate all account-specific data. Atomic Learning provides customer level user management per customer via a secure user management interface from within the Atomic Learning website.

Atomic Learning assessments are taken on a SSL encrypted website for only the user of that session to see. Atomic Learning saves the results of the assessments to a database owned and managed by Atomic Learning. Only privileged Atomic Learning employees or privileged customer user accounts can report on assessments taken for that customer.

Atomic Learning saves the results of learning object views for each individual user account to a database owned and managed by Atomic Learning. Only privileged Atomic Learning employees or privileged customer user accounts can report on tutorial views for that customer.

Customer account management is only allowed to Atomic Learning employees though a separate interface outside of Atomic Learning's website. Strict access is maintained on the customer account management interface for Atomic Learning employees at all times.

6. ## How is data protected in transit?
   Data is protected in transit by SSL.

7. ## Does Atomic Learning perform background checks on personnel with administrative access to servers, applications and customer data?
   Yes, Atomic Learning performs background checks on all employees prior to hiring.

8. ## Does Atomic Learning subcontract functions such as analytics?
   No.

9. ## What is Atomic Learning's process for authenticating callers and resetting access controls, as well as establishing and deleting accounts?
   The process for resetting access controls may entail two options. In most cases, users are directed to a password reset page of the Web site. Upon entering their email address, the system verifies the address as a valid account and automatically sends a password reset link to that email address. In some instances of phone support, Atomic Learning staff may enable the password reset function for a user who has forgotten a password. In such a case, the system automatically sends a password reset to the associated email address of the user. In the rare event that a user does not have an email address associated with the account, the password reset link will be sent to the email address listed as the administrative access for the account. At no point will Atomic Learning staff have access to view a user password. This information is encrypted and not accessible to Atomic Learning staff.

   In some instances, to provide trouble-shooting to a user seeking support, Atomic Learning account management and support staff will assume an administrative role that allows staff to masquerade as a user. This step is only taken following verbal or written consent by the user and the Atomic Learning staff will, at no time, have access to the user's password.

   Accounts are not deleted, but rather deactivated.

10. ## If student or other sensitive data is transferred to the provider, are all uploads via SFTP or HTTPS?
    Customers are instructed to transmit user data through an upload tool that uses HTTPS or through SFTP.

11. ## What are Atomic Learning's security protocols?
    Atomic Learning uses enterprise class firewalls and intrusion detection systems. Atomic Learning employs around-the-clock monitoring to detect potential security threats to the site. Atomic Learning

performs quarterly vulnerability, penetration and intrusion prevention testing to access infrastructure security. Atomic Learning addresses potential systems security vulnerabilities through necessary updates and patches.

Atomic Learning user account authentication is secured on a SSL encrypted website and/or application.

12. Are all of the network devices located in secure facilities and under controlled conditions?

Atomic Learning collocates their servers and network systems in two data centers in the Minneapolis, Minnesota metropolitan area. The data centers are approximately 20 miles apart, on separate power grids and connected to separate Internet backbones heading opposite directions. Public Internet service is multi-provider. Both data centers have redundant backup generators and power supplies. Each data center is configured with server load balancing technology to accommodate for server failure. A redundant route private connection links the two data centers to provide replication and interconnectivity.

In order to maintain the highest levels of infrastructure efficiency and uptime, Atomic Learning employs several strategies to maintain the health of its site infrastructure.

Alerting: An alerting system is used to monitor server and network health metrics. This system keeps Atomic Learning informed around the clock and alerts their technical staff if system metrics fall outside of prescribed ranges. Some of the metrics include (but are not limited to): server CPU utilization, server network reachability, data center reachability, web port reachability, and server load.

Monitoring: In order to proactively build system infrastructure to ensure they remain ahead of demand, Atomic Learning carefully monitors and records several metrics over time. The metrics Atomic Learning watches are similar to those monitored by the alerting system, but are graphed so that Atomic Learning is able to see trends over time and react to them as needed. Active monitoring allows Atomic Learning to assess our site response times and view site load times.

13. Are backups performed and tested regularly and stored off-site? How are they secured?

Atomic Learning collocates their servers and network systems in two Tier 4 data centers to achieve fault tolerance. Atomic Learning uses redundant web servers and load balancing, and utilizes offsite redundant DNS servers and services. Atomic Learning employs database replication over a private connection between data centers.

If a server fails, a load-balancing device detects the failure and stops sending traffic to the failed device. The load-balancing device then automatically removes that server from the site. In the event of a single server failure to one of our servers at our primary data center, we do not fail over to our backup data center, but proceed to load balance the website at the primary data center on the remaining servers in that server pool. In the event that more than one server in the pool has a failure at our primary data center, we then fail over our site to our backup data center.

Atomic Learning has a server at a server hosting provider, in a Los Angeles, California data center. Atomic

Learning hosts their public primary DNS servers on this server. The hosting service provides redundant power, HVAC systems, and their network uptime is guaranteed at 100% availability. The provider has support available for Atomic Learning to contact 24/7. For DNS fault tolerance, Atomic Learning has secondary and tertiary DNS servers hosted at the primary data center and at Atomic Learning's corporate office.

Atomic Learning has a primary database server at our primary data center replicated to a secondary server at our backup data center. If the primary database server fails, we fail over to the secondary database server at the backup data center.

14. Are software vulnerabilities patched routinely or automatically on all servers?

Automated patching systems are used to address security vulnerabilities.

15. What is the policy for deleting collected information?

Data is deactivated, rather than being deleted. Deactivated data is accessible to only the Atomic Learning system administrator. Data can be fully deleted upon request.

16. Is "live" student data used in non-production environments?

Only deactivated data is used in non-production environments.