Woodcock-Johnson® and Woodcock-Muñoz Language Survey®–Revised Normative Update Technical and Data Security Overview

Houghton Mifflin Harcourt - Riverside (HMH - Riverside) is pleased to offer online scoring and reporting for *Woodcock-Johnson® IV (WJ* IV*)* and *Woodcock-Muñoz Language Survey®–Revised Normative Update* (*WMLS-R NU*). With online scoring and reporting, examiners can enter raw scores for any test in the *WJ* IV suite of assessments and receive reports for all derived scores and clusters. Our online system offers benefits to users of the *Woodcock-Johnson* Suite of Assessments such as 24/7 secure access to data, real-time results, robust reporting, and coming late 2014, offline scoring capabilities through mobile apps. We and our vendors take all reasonable precautions to protect information and data, both physically and online. We use the latest solutions to defend our servers and protect our customer's data accordingly to meet regulatory compliance.

Our secured servers are hosted with our partnered vendor located in a secure, location in Andover, Massachusetts. . Our partnered vendor's data centers meet the highest security standards in the industry for data integrity and related processes. This includes physical access to the data center and other sensitive areas; logical authentication and access to networks, programs, and data; monitoring to proactively identify and fix system vulnerabilities; and systems implementation to ensure infrastructure changes are accurate and logged. In addition, our partnered vendor's SSAE-16-certified U.S. data centers meet the highest security standards for cloud-enabled data and application integrity.

Physical Security

All production servers are hosted at a secure hosting facility and physical access is limited to approved personnel only. Data centers are monitored from two global network operations centers. Physical access to data center facilities is restricted. Entering the building that houses the data center requires mandatory visitor registration, visitor escorts, employee badge access, and biometric palm scanner authentication. In addition, video surveillance is monitored 24 hours a day, seven days a week.

Physical Security and Cloud Computing Environmental Safeguards

Our partnered vendor also has sophisticated monitoring devices in each facility: early-warning fire detection, smoke and temperature detectors, and 24/7 digital video surveillance. Full data-grade HVAC systems are in place to regulate air temperature and humidity. Security also extends to management. Role-based access control ensures that each user has only the permissions required for their role. Permissions can also be set on objects or groups managed by our partnered vendor. All activity is logged for auditing purposes.

Equipment Repairs

Equipment repairs are done on site at the hosting facility. If hardware needs to be sent back to the manufacturer, we will migrate your data onto a new server and wipe all data and operating systems off of the server before sending out for repair or replacement.

Operating System

Houghton Mifflin Harcourt recognizes that the data in our system is of immense value to customers. To ensure that our customers' data is safe not only during day-to-day operations but also during releases of updates to the application, we ensure that all procedures meet the highest standards of quality.

Software Updates

We regularly patch our software to ensure our operating systems and any other software running on our servers contain the latest security patches.

Permissions and Privileges

Only personnel with the appropriate authority will have controlled access to the application and data file servers. This is enforced through the use of permissions, passwords, and unique IDs.

Monitoring and Anti-Virus

Lumension® Endpoint Management and Security Suite software is used to monitor and protect our servers. This software expands our operation visibility with delivery of a more effective IT security standard on all HMH servers that protect our systems from the following:

- Ensures complete protection against all known malware, including viruses, Trojans, rootkits, spyware and adware.
- Provides additional layers of defense against zero-day malware through sandboxing and exploit detection technology.
- Provides granular settings to ensure endpoint performance and user productivity is not impacted by AV scans.
- Delivers a scalable and efficient defense against well-known and fast-spreading malware.
- Application role level security.
- HMH will work with state agencies to ensure that the appropriate level of access for an individual role is configured, e.g., teachers can only see their assigned student data. Administrators at a school level can only access data pertaining to their school, etc.

Only Houghton Mifflin Harcourt employees who need the information to perform a specific job are granted access to personally-identifying information and data. Sign-on passwords are required of Houghton Mifflin Harcourt's staff and are changed every 90 days in accordance to HMH security policy. All of HMH's employees are informed of and subject to corporate confidentiality, security and privacy guidelines.

Our online testing systems are configured so that all logins are made using the SSL (Secure Sockets Layer) 128-bit encryption standard communications. Our applications use SSL (Secure Sockets Layer) standard communications. Sign-on permissions, passwords, unique IDs or a combination of these measures are required in order to limit access to the application and database servers to appropriate state personnel, such as teachers, examiners and administrators. For example, our systems are configured so that teachers can access only their assigned students' data and administrators can access data pertaining to their schools. Data will be expunged upon the request of the customer.

All personally identifiable information is encrypted upon access through the web interface through the use of SSL technology in addition we apply the SSL cert to the actual server instead of the load balancer which increases the security of our product.

Network-Intrusion Detection and Prevention

All traffic is carried on secure VLANs, passing through a firewall to access other cloud VLANs or physical networks. Our partnered vendor's advanced firewall technology also provides intelligent threat defense with identity-based access control and denial-of-service-attack protection.

Firewall Services and Two-Factor Authentication

A shared firewall ensures segregation of VLAN traffic terminating on the same physical segment. A virtualized firewall gives you your own individual security contexts on an enterprise firewall appliance. And each cloud customer has their own dedicated firewall appliance.

File Integrity Services

Our partnered vendor uses Trip Wire's file-integrity services to assess integrity on customer virtual machines. File integrity services monitor both file and configuration integrity – looking at raw file contents, permissions, registry settings, and security settings.

Data Integrity

Our partnered vendor maintains back-up data both on and off-site to accommodate rapid recovery of recent data as well as long-term off-site storage. They store tapes in a secure location within each data center and follow airtight security procedures for sending tapes to secure offsite locations transported via armored truck.

Production Data Redundancy

Customer data stored in the database is clustered, so if one cluster is unavailable, data will be pulled from another.

Backup Process

All servers and databases are backed up on a regular basis, including full database backups each Sunday and differential backups several times daily. In addition, a full monthly backup including the database and operating system is performed at the end of each month, which is then stored at an offsite secure location in a fireproof vault. All monthly tape backups are held off premises for 13 months in a secure, environmentally controlled facility. All weekly full backups are stored in the same off-site facility for a period of 5 weeks. As necessary, the hosting facility will restore any files or directories as requested. The time for restoration varies depending on the size of the files and length of time since deletion. In the event of a catastrophic failure, the database backups will be made available through file transfer and/or SDLT tapes can be delivered to our secondary hosting facility where functionality to the system would be restored within hours.

Power and Environment

Our partnered vendor's data centers are powered through highly redundant and efficient systems backed by generators that can keep the site fully operational at full load for 24 hours with hot-refuel capability, without any power from the electric grid. The parallel UPS systems and battery backup are redundantly supplied by diversely distributed utility. The diverse power routes and redundant switching infrastructure help ensure your connections are performance-optimized.

- ***Green Advantage***

  Our partnered vendor is a member of the Green Grid, a global consortium of leading IT organizations focused on data-center efficiency, ensuring its data centers minimize power consumption. They deploy energy-efficient technologies like virtualization and use energy-efficient servers, storage, and networking equipment to offer us an energy-efficient, green environment. Their equipment and proprietary monitoring software cut energy consumption of our cooling systems by more than 20 percent.

- ***Precision Environment***

  The data center is completely equipped with data-grade HVAC systems with N+1 redundancy for regulating air temperature and humidity where our equipment resides. This helps ensure longer life and continuous operations for our equipment.

Recovery Process

The recovery process for client data uses standard data extraction and import utilities. Most often, database archives can be simply restored using the standard SQL import facility, where the file created by the daily backup re-creates all the tables and relations between them and then inserts the data. As part of the normal development and testing process, the daily backup file is routinely copied and imported. This enables HMH to ensure the integrity of production backups and the backup process.

Uptime

HMH provides consistent access to the *WJ* IV*;* however, the *WJ* IV platform does undergo occasional routine maintenance. Your district or organization will be notified in advance of any scheduled system downtime outside the maintenance window that impacts their use of the system.

For More Information

For more information on *Woodcock-Johnson* IV, *Woodcock-Muñoz Language Survey®–Revised Normative Update* or any HMH – Riverside product, please contact your local representative or visit http://www.hmhco.com/assessment-professionals/assessment-solutions .