



Riverside Score[®]: Our Security Commitment

At Riverside Insights[®], safeguarding examinee data isn't just a priority; it's our duty. As your trusted partner, we understand the critical importance of preserving the confidentiality and integrity of student information.

Here's how we go above and beyond to fortify our defenses and ensure the protection of your data:

Single Sign-On (SSO):

Provides seamless access to our platform using existing credentials. With SSO, examiners enjoy streamlined authentication, reducing the risk of unauthorized access.

Multi-factor authentication available (MFA) with SSO:

By requiring multiple forms of verification, such as passwords and unique codes sent to mobile devices, we bolster our protections against unauthorized access, safeguarding student data with an extra layer of security.

Data De-identification:

We recognize the sensitivity of student data and the importance of preserving privacy. Robust de-identification techniques are used to anonymize personal data while retaining its utility for educational purposes. By de-identifying data, we protect student privacy without compromising the integrity of educational insights.

Encryption:

We protect data by ensuring that only parties with authorized credentials can access it. Personal information hosted in Riverside Score is encrypted in transit (TLS 1.2 or later) and at rest (AES 256).

Annual Audits & Vulnerability Testing:

Transparency and accountability are paramount in our security practices. An annual SOC-2 audit helps us identify and address high-priority security vulnerabilities, ensuring that our platform adheres to the highest standards of data security and regulatory compliance.

Cybersecurity Training

Our employees play a pivotal role in cybersecurity and have been equipped to recognize, respond to, and prevent cyber incidents by completing cybersecurity training upon hire and annually thereafter. We also provide incident response and ethics training and conduct periodic phishing simulations to reinforce best practices.



Riverside Score[®]: WJ V Data Security Commitment

When Woodcock-Johnson[®] V (WJ V[™]) customers entrust us with their data, *Riverside Insights* treats that responsibility with the utmost seriousness. We dedicate considerable resources and efforts to ensuring that customer data is secure and is only used for permissible purposes.

Here's an in-depth look at the comprehensive security program protecting WJ V users:

Secure Software Development Lifecycle:

We follow a secure software development lifecycle process (SDLC) to deliver high quality and secure technology solutions. This process involves automated scanning of code to catch vulnerabilities before they can impact the platform.

Penetration Testing:

To see how our platform holds up against potential cyber-attacks, we engage a third-party service provider to penetration tests, or simulated cyberattacks annually. We review the results of the test and incorporate the feedback to make the platform more secure.

Endpoint Protection:

In today's digital work environment, every endpoint, such as a laptop or server, can be an avenue for cyber threats. Riverside deploys an endpoint protection solution from a leading provider to guard our endpoints against malicious activity.

User Access Reviews:

We stay on top of who has access to your data by conducting quarterly user access reviews. Access permissions are promptly updated based on those reviews.

For inquiries about our security measures or to learn more about how we can protect your organization's data, please don't hesitate to reach out to us at compliance@riversideinsights.com

Riverside Insights – Protecting Your Data, Empowering Educational Excellence