GL Education®
A Renaissance Company

Information Security Overview

As a leading provider of assessments and analytics to schools and school groups worldwide, information security is a critical aspect of GL Education's business. We abide by our regulatory obligations and strive to exceed the expectations of the schools we serve. Every day, thousands of users depend upon our commitment to protect their data. We take this commitment seriously.

This Information Security Overview describes the ways in which we protect your data. GL Education may update or modify these security measures from time to time provided that such updates and modifications do not materially decrease the overall security of the relevant personal data.

Technical Controls

Data Storage & Hosting

GL Education's assessments and analytics are designed around the core pillars of confidentiality, integrity and availability. Its products are developed, tested, and deployed in Microsoft Azure and Amazon Web Services (AWS) across several geographically and logically separated locations. Microsoft Azure complies with an array of industry-recognised standards including ISO 27001 and SOC 2.

Microsoft Azure Hosted Products:
Testwise, WellComm

Please visit Azure Global Infrastructure for more information.

Amazon Web Services (AWS) Hosted Products:
GL Ready

Please visit AWS Global Infrastructure for more information.

Data Location & Sub-Processors

See our list of Sub-Processor information.

Credentials and Role-Based Access

Each school has a unique identifier within GL Education products. Each user is assigned unique login credentials, which must be authenticated before the user can access the school site. Users are assigned to distinct roles, such as student, teacher, or administrator, which limits what information users can access or edit.

© 2024 Renaissance Learning, Inc. All rights reserved. | www.renaissance.com

Encryption

Data encryption is an important component of the protection of sensitive data. GL Education's team works with its parent company, Renaissance, to review and update encryption controls based on the latest standards and guidelines published by Open Web Application Security Project (OWASP) and National Institute of Standards and Technology (NIST).

- *In transit:* GL Education requires encryption over public connections, using Transport Layer Security (TLS), commonly known as SSL, using industry-standard protocols, ciphers, algorithms, and key sizes. The current standard is TLS 1.2 or better.
- *At rest:* GL Education requires encryption using industry standard Federal Information Processing Standards (FIPS) approved encryption algorithms. The current standard is AES 256 or better.

Cybersecurity Features

GL Education implements layered security controls to protect customers' data. These include Endpoint Detection and Response software and services; next-generation firewalls; segmented design; patching; system hardening processes; and several vulnerability scanning techniques. The Information Security team collects and analyses an array of log data including system logs, system security configuration logs, access control logs, system process analysis, network traffic analysis, and network bandwidth consumption. We monitor systems 24 hours a day, 7 days a week, and any suspicious activity is promptly investigated.

Application Security Testing

Dynamic Application Security Testing (DAST) is run against our key applications on a regular basis. The DAST process, which is an integral piece of our software development cycle, tests our software for exploitable weaknesses and vulnerabilities at each stage of the development process.

Penetration Testing

GL Education engages with a third party to conduct penetration tests on each application and its underlying infrastructure annually. Penetration test results are used to validate all the security controls we have implemented. All penetration test findings are assessed and remediated through our change management processes and product deployment pipelines.

Business Continuity & Disaster Recovery

GL Education maintains and tests Business Continuity and Disaster Recovery plans to protect your data. Backups are protected using segmentation and vaulting technologies. Additionally, services are deployed into scalable groups and are load balanced across compute and storage services running in geographically diverse availability zones to provide high availability and reduce the risk of service outage. GL Education also manages all of its cloud infrastructure as code, which facilitates quick recovery or rollback in case of outage, and better transparency into changes in infrastructure over time.

Physical Controls

GL Education's digital products are powered by Microsoft Azure or Amazon Web Services (AWS): both durable technology platforms that align to an array of industry-recognised standards. Both services and data centers have multiple layers of operational and physical security. For more information, please visit https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security or https://aws.amazon.com/compliance/data-center/controls/

Administrative Controls

Risk Management and Governance

GL Education's parent company, Renaissance, has designed its security program to substantially follow the FIPS 200 standard and NIST Special Publication 800-53. Renaissance also assesses its Information Security program against the Center for Internet Security (CIS) Top 18 Controls and the NIST Cybersecurity Framework (CSF).

Cybersecurity Risk Committee: The Renaissance Cybersecurity Risk Committee is charged with identifying, tracking, and managing cybersecurity risks. The committee communicates with executive leadership and the board of directors to keep them informed of key cyber and business level risks facing Renaissance. The Committee is also charged with evaluating Renaissance information security and privacy policies, procedures and operations along with Renaissance's products, product development, and product deployment systems to identify potential areas of vulnerability and risk. These evaluations are used to develop policy, practices, and processes aimed at mitigating or removing vulnerabilities and risks. The Committee assesses all observed and perceived risks to develop policy, practices and priorities to manage risk to an acceptable level.

Incident Response Team

We maintain an Incident Response Plan and have a standing Incident Response Team. The Incident Response Team performs Tabletop Exercises at least twice annually. Tabletop Exercise results are used to further refine the Incident Response Plan, policy, and risk management practices.

The Information Security team collects and analyses an array of log data including system logs, access control logs, system process analysis, network traffic analysis, and network bandwidth consumption. Monitoring and analysis of collected data occurs 24 hours a day, 7 days a week and any suspicious activity is promptly investigated and reported to responders.

Our employees are obligated to protect all customer data. This includes reporting any suspected or known security breaches, theft, unauthorised release, or unauthorised interception of customer data. Should evidence of an information security incident arise, our Incident Response Team will initiate the response plan.

We encourage customers with any questions or concerns regarding security or related issues to contact our Data Protection Officer at **dpo@gl-education.com**

Security Education, Training & Awareness

All employees are required to complete Privacy and Information Security training on an annual basis. The GL Education and Renaissance IT and Security teams regularly communicate information about the current cybersecurity threat landscape to all employees. Additionally, Renaissance conducts an anti-phishing and social engineering awareness and training program. Supplemental training events, such as International Privacy Week and Cybersecurity Awareness Month, are also major elements of the training program.

Compliance

Audits: Renaissance's enterprise Information Security & Compliance Program successfully completed the SOC 2 Type 2 examination of controls in August 2023. The examination is formally known as a Type 2 Independent Service Auditor's Report on Controls Relevant to Security, and reports on Renaissance's systems and the suitability of the design, implementation, and reporting of our information security controls. Our SOC 2 Type 2 is scoped to specific products and services. For more information on our SOC audits, including which products have completed SOC audits, please see our Trust Center: https://trust.renaissance.com.

GL Education was not scoped in the 2023 SOC 2 Type 2 examination of controls. GL Education will be included in the 2025 SOC 2 Type 2 examination of controls. Please contact our Data Protection Officer for more information: **dpo@gl-education.com**

Employees: All employees are required to read, sign, and agree to abide by Renaissance's Information Security and Information Technology policies. Background checks are conducted as part of the onboarding process for employees to the extent permitted by law.

Vendors/Sub-processors that Support Our Products: Renaissance maintains a vendor compliance program. Vendors' security and privacy practices are reviewed and analysed. Additionally, Renaissance enters into written contracts with each vendor/sub-processor containing terms that offer similar levels of data protection obligations and protection for customer personally identifiable information as identified in our Data Protection Addendum with customers.

If you have specific information security questions, please contact: **dpo@gl-education.com**

© 2024 Renaissance Learning, Inc. All rights reserved. | www.renaissance.com