DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

RENAISSANCE

Information Security Overview

Welcome educators! As a leading provider of technology products to K–12 schools worldwide, information security is a critical aspect of Renaissance's business. We abide by our regulatory obligations and strive to exceed the expectations of the educators we serve. Every day, millions 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. If you are interested in learning more about how we handle the privacy of your data (data use, collection, disclosure, and deletion) please visit our Privacy Hub for more information.

Technical Controls

Data Storage & Hosting

Cloud-Hosted Products:

Renaissance cloud products are designed around the core pillars of confidentiality, integrity, and availability. Renaissance products are developed, tested, and deployed in Amazon Web Services (AWS) and Google Cloud Platform (GCP) across several geographically and logically separated locations. AWS and GCP comply with an array of industry recognized standards including ISO 27001 and SOC 2.

Amazon Web Services (AWS) Hosted Products:
Renaissance Growth Platform, Freckle, myON, Schoolzilla, Star Phonics, Lalilo, EduClimber, FastBridge, eSchoolData

For more information about AWS, please visit https://aws.amazon.com/about-aws/global-infrastructure/.

Google Cloud Platform (GCP) Hosted Products:
SchoolCity, DNA, EduClimber

For more information about GCP, please visit https://cloud.google.com/infrastructure/.

Renaissance Data Center:

The Renaissance Data Center (RDC) serves our international Renaissance Place customers and is located in Wisconsin, USA. Renaissance Place runs on dedicated servers, network infrastructure, and data stores. Each customer's data is stored in a separate database that operates independently of all other customers' databases. Each school or trust that uses Renaissance Place has its own unique Renaissance hosted site URL, and each user is assigned unique login credentials.

Data Location & Vendors/Sub-Processors

See our list of Sub-Processor information.

Encryption

Data encryption is an important component of the protection of sensitive data. Renaissance's security team consistently reviews, and updates 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:* Renaissance requires encryption over public connections, using Transport Layer Security (TLS), commonly known as SSL, using industry-standard protocols, ciphers, algorithms, and key sizes.
- *At rest:* Renaissance requires encryption using industry standard Federal Information Processing Standards (FIPS) approved encryption algorithms.

Credentials and Role-Based Access

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

Cybersecurity Features

Renaissance implements layered network 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. Renaissance collects and analyzes 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 all our 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

Renaissance 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've implemented. All penetration test findings are assessed and remediated through our change management processes and product deployment pipelines.

Business Continuity & Disaster Recovery

Renaissance 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. Renaissance also manages much 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

Cloud-Hosted Products:

Renaissance cloud products are powered by AWS and GCP: durable technology platforms that align to an array of industry-recognized standards. AWS and GCP services and data centers have multiple layers of operational and physical security.

For more information about AWS, please visit https://aws.amazon.com/about-aws/global-infrastructure/.

For more information about GCP, please visit https://cloud.google.com/infrastructure/.

Renaissance Data Center:

The Renaissance Data Center, which hosts the international Renaissance Place product, is located at Renaissance's corporate headquarters in Wisconsin. Entry into Renaissance properties is controlled via employee magnetic key entry.

Only Cloud Operations and Network Services personnel who are responsible for management of data center infrastructure are allowed unescorted access to the Renaissance data center. Admittance to the data center itself is controlled through a proximity card access system and a motion-based detection system. All visitors to the data center, as well as their internal employee escorts, must sign an access log. We also monitor log files, review access logs, track system usage, and monitor network bandwidth consumption.

The environmental conditions within the data center are maintained at a consistent temperature and humidity range, with a third-party security firm monitoring conditions within the data center. Should any changes in power or temperature occur, key Renaissance personnel are notified. Electrical power is filtered and controlled by dual uninterruptible power systems. If a power outage occurs, an automatic-start generator provides uninterrupted power to our servers and heating, ventilation, and air conditioning units. A waterless fire protection system and an early-warning water detection system help to prevent damage to the servers that store our customers' data.

Administrative Controls

Risk Management and Governance

Our security processes and controls substantially follow the FIPS 200 standard and NIST Special Publication 800-53. Renaissance also assesses its Information Security and Privacy programs 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

Renaissance maintains an Incident Response Plan and has 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.

Renaissance collects and analyzes 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.

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

We encourage district representatives with any questions or concerns regarding privacy, security, or related issues to contact our Chief Information Security Officer via e-mail at infosecurity@renaissance.com.

Security Education, Training & Awareness

All Renaissance employees are required to complete Privacy and Information Security training on an annual basis. Renaissance regularly communicates 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 1 examination of controls in November 2022. The examination is formally known as a Type 1 Independent Service Auditor's Report on Controls Relevant to Security, and reports on Renaissance's systems and the suitability of the design of our controls. Our SOC 2 Type 1 is scoped to specific products and services. For more information on our SOC audits, including which products have completed SOC audits, please contact infosecurity@renaissance.com.

Renaissance's enterprise Information Security & Compliance Program intends to complete a SOC 2 Type 2 examination of controls in 2023 and annually thereafter.

Employees: All Renaissance employees must sign a nondisclosure agreement prior to the start of their employment. Additionally, 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 analyzed. 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: **infosecurity@renaissance.com**