Summit Learning Security Whitepaper

Security at Summit Learning

Protecting data privacy is a top priority for Summit Learning. Our Program Agreement and our Data Privacy Addendum solidify the commitments that Summit Learning and schools make to each other, including our security and privacy commitments.

Summit Learning partners with the Chan Zuckerberg Initiative (CZI), a philanthropic organization that supports Summit Learning by pairing pro bono technology expertise with educators to help develop free tools that empower teachers to better meet students' individual needs and interests in the classroom.

As part of the partnership, CZI supports the Summit Learning Platform, which is an online tool that is part of Summit Learning. In order to fulfill those responsibilities, a limited number of CZI staff members who support Summit Learning need access to student, teacher and parent data. Privacy and security are top of mind for this partnership: CZI staffers working on the Summit Learning Platform follow the same rigorous Data Privacy Addendum that Summit Learning commits to with our partner schools. Data is used for educational purposes only and will not be sold. You can learn more about our relationship with CZI and the other service providers we use to host and deliver the Summit Learning Platform on our Privacy & Security FAQs.

This page is designed to provide technical readers, such as Chief Information Officers or Chief Technology Officers at our partner school districts, additional clarity and specifics about how we act on our commitments made in the legal agreements. While this document is written for technology experts who often play a key role in assessing our policies, we recognize that data privacy is just as important to families, teachers, and students as it is to school officials. If you would like to find out more and access materials that are written to help you digest the more technical information here, please visit our dedicated Privacy Center.

Our information security program implements and maintains controls that align to the Center for Internet Security Critical Security Controls. We regularly evaluate our policies and practices to improve security and to keep up with latest practices of the security industry.

Should you have security or privacy questions, please reach out to our team at privacy@summitlearning.org.

Infrastructure Security

Encryption at Rest and In Transit

Access to the Summit Learning Platform occurs via encrypted connections[1] (HTTP over TLS, also known as HTTPS) which encrypt all data before it leaves Summit Learning Platform's servers and protects that data as it transits over the internet. We use HTTP Strict Transport Security to ensure that pages are loaded over HTTPS connections and our TLS configuration receives an A+ from Qualys SSL Labs. All personally identifiable information is encrypted at rest using modern encryption algorithms such as AES-256 or stronger.

Network Security

The Summit Learning Platform uses Amazon Web Services (AWS) and Heroku, two leading cloud providers, to host the infrastructure. Both providers undergo strict ongoing security assessment from external audit firms to ensure compliance with security standards including ISO 27001, SOC 2, PCI DSS Level 1, and FISMA. See https://aws.amazon.com/compliance/programs/ and https://www.heroku.com/compliance for more details.

Network access to the Summit Learning Platform's infrastructure is highly restricted. AWS hosted infrastructure resides in a dedicated Virtual Private Cloud (VPC) which is designed to ensure that only authorized traffic over approved ports is allowed. Development infrastructure resides in a separate VPC. We leverage built-in AWS services, such as AWS GuardDuty, to monitor for suspicious activity. Heroku hosted services utilize Heroku Private Spaces to provide similar network isolation.

Patching

We use automated processes to regularly install security updates on the infrastructure that powers the Summit Learning Platform, these processes include:

- **Heroku**: Patching is automatically handled by Heroku.
- **AWS Managed Services (e.g. Relational Database Service):** AWS proactively notifies our engineering team when updates are available and we apply them in a timely fashion.
- **AWS EC2:** All EC2 instances are configured to automatically apply operating system and kernel patches. This includes automatic restarts as needed.

[1] Note: Some schools implement content monitoring and filtering technologies that may involve the school decrypting Summit Learning Platform content.

Access Management

Access to the Summit Learning Platform infrastructure is highly restricted. We limit access to individuals who need access to do their jobs such as engineers, data scientists, product managers, and support personnel. All access to our infrastructure is logged. All access to our infrastructure requires the use of strong passwords and multi-factor authentication.

Backups

We have a data backup and recovery capability that is designed to provide a timely restoration of the Summit Learning Platform, with minimal data loss, in the case of catastrophic failure. These backups are encrypted and stored in a different region than production databases.

Physical Security

The Summit Learning Platform is currently hosted in Amazon Web Services (AWS), which employs industry-leading physical security measures to protect their data centers such as a full 24/7 onsite security team, video surveillance, and perimeter intrusion detection systems. These security features are regularly audited by third-party auditors. You can learn more about AWS' physical security here.

Application Security

Secure Software Development Lifecycle

In addition to designing our systems with privacy and security in mind, we employ a combination of manual and automated processes to identify potential vulnerabilities. This includes mandatory code review, automated source code scanning, automated dependency scanning, as well as periodic reviews of the Summit Learning Platform by external security experts. In addition, we run a Vulnerability Disclosure Program through our partnership with BugCrowd, which allows security researchers who identify vulnerabilities to responsibly disclose them to us.

If you suspect or know of a security vulnerability in the Summit Learning Platform, please contact us at security@summitlearning.org.

Browser Security

We use an up-to-date Content Security Policy (CSP) to prevent unauthorized JavaScript from running in the context of the Summit Learning Platform and we use standard countermeasures to protect against Cross-Site Request Forgery (CSRF).

Authentication

The Summit Learning Platform exclusively uses Single Sign-On via Google G Suite or Microsoft Office 365 to authenticate students, teachers, and other school staff. This means that passwords for students, teachers, and other school staff are managed by their school and are never available to us.

Parents and guardians who access the Summit Learning Platform use usernames and passwords which are protected using industry standard methods, including per user salted non-reversible password hashing. We utilize bcrypt to hash parent and guardian passwords.

All Summit Learning Platform staff access the Summit Learning Platform using Single Sign-On systems which require strong passwords and multifactor authentication.

Access Control

The Summit Learning Platform has a role-based access control system which puts schools in control of who has access to data. School administrators control which teachers, students, and parents are authorized to access data within the school. In addition, school administrators select site-specific data privacy permissions for their teachers as is appropriate to their particular school environment.

Staff who work on the Summit Learning Platform are also subject to access controls which limit their access only to the data reasonably needed to do their job. All Summit Learning Platform access, including access by Summit Learning staff, follows established procedures and is logged. Logs themselves are further protected to ensure their integrity.

Security Governance and Policies

Incident Response

We have an established process that is followed whenever we detect suspicious or abnormal activity on the Summit Learning Platform that might have a security implication. In order to support this process and our efforts to ensure that the Summit Learning Platform is available, our engineering and security teams have on-call rotations to provide a designated point person available to respond to any suspicious or abnormal activity.

As part of our incident response process, we perform post-mortem reviews of major incidents including both security and non-security related (such as site outages). These post-mortem reviews are designed to ensure that we learn from past incidents and if needed, improve the Summit Learning Platform to prevent them from occurring again in the future.