# Security Whitepaper

Last Updated: October 13, 2020

## Along Security Principles

Along is offered by Gradient Learning and is being developed with input from teachers, students, school leaders, and our technology partners from the Chan Zuckerberg Initiative (CZI). Gradient Learning also operates the Summit Learning program, where strong partnerships with schools and educators begin with a commitment to transparency, privacy and security.

Along embeds these same values in its design, development, and operation, and is currently being piloted in several school districts. We've outlined our commitments to educators, students and parents in our Privacy Policy, User Agreement, Code of Conduct, and this Security Whitepaper. Should you have security questions or concerns, please reach out to the Along team at security@comealong.org.

## Overview

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.

Gradient Learning uses several Service Providers to host and deliver Along which are listed in our Third Party Service Provider List. Any CZI staffers working on Along that need access to student, teacher, or parent data follow the same rigorous Data Privacy Addendum that Along commits to its users.

**We do not make money from students and teachers using Along, nor do we allow ads to be placed on Along. We do not and will never sell or rent student and teacher personal information.**

# Infrastructure Security

## Encryption at Rest and In Transit

Access to the Along service occurs via encrypted connections (HTTP over TLS, also known as HTTPS) which encrypt all data before it leaves Along'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

Along 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 AWS' Compliance Programs and Heroku's Compliance Programs for more details on their respective security programs. Network access to the Along 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. Along's 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 Along, 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.

## Access Management

Access to the Along 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 multifactor authentication.

## Backups

We have a data backup and recovery capability that is designed to provide a timely restoration of Along, 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

Along 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 Along 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 Along product, please contact us at security@comealong.org.

## Browser Security

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

## Authentication

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

All staff who work on Along use Single Sign-On systems which require strong passwords and multifactor authentication.

## Access Control

Along data models and authorization methods enforce strong access control for student-teacher communication. Only a student's authorized teacher can interact with that student's data, and students cannot see each other's content.

Staff who work on Along are subject to access controls which limit their access only to the data reasonably needed to do their job. All Along access 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 Along that might have a security implication. In order to support this process and our efforts to ensure Along 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 Along to prevent them from occurring again in the future.