DATA PRIVACY AND SECURITY PLAN

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

DATA SECURITY AND PRIVACY PLAN

Vendor's DATA SECURITY AND PRIVACY PLAN is as follows:

Remind collects a small amount of PII, including but not limited to, phone number, email, name, birthday etc. Remind uses this information to provide the core messaging service to our users. We have gone to great lengths to collect only the data we need, to protect that data to the best of our ability and to ensure users and schools can control that data as they see fit and to comply with regulation at the local, state and national level.

Data in transit

- All data transferred in or out of our data centers (AWS VPC) is encrypted using Transport Layer Security (TLS), using strong cipher suites. Termination of TLS connections is handled by AWS ELB using the most recent recommended Security Policy. In cases where TLS is not an option, appropriate transport level encryption mechanisms are used, such as SSH or IPsec.
- We follow industry standard best practices for web application security, such as flagging authentication cookies as secure, enabling HTTP Strict Transport Security (HSTS), and protecting the application from Cross-Site Request Forgery (CSRF) attacks that could be used to steal or otherwise modify user data.

Data at rest

- Databases and backups are encrypted at rest with AES-256 bit encryption.
- Passwords for users of Remind are stored in hashed form using an industry standard cryptographic hash function called bcrypt.

Key/Secret management

- All encryption keys are stored on a FIPS 140-2 validated Hardware Security Module (HSM) managed by AWS KMS. No employee has direct access to the private key material for any encryption key. By default, we restrict access to decrypt data to a small subset of employees. By default, applications and services are only given access to decrypt data that they explicitly need.
- All SSL/TLS certificates are managed using AWS ACM, and no employee has access to the private key material.

- SSH access to servers requires access to our VPN, and requires an SSH key signed by our internal Certificate Authority. Only a small subset of employees are given SSH access, which is automatically revoked after a period of time (24 hours). Employees with SSH access follow best practices to secure their private SSH keys.
- When possible, we use short time constrained credentials when accessing data to mitigate against accidental credential exposure.

Access controls

- Databases are only accessible within our internal network (AWS VPC) in addition to requiring database credentials (username/passwordof a database user). Different types of data are shared across separate databases, and access to databases has process level isolation.
- Employee access to data containing PH requires access to our VPN, as well as access to our internal platform-as-a-service. Both systems require Multi-Factor Authentication (MFA), and access is automatically revoked after 24 hours. All access is logged and periodically audited.
- Employee access to our AWS accounts requires the use of MFA, and access is revoked after 24 hours. Employees are assigned to specific roles that give them only the access they need. By default, no engineer has access to databases or S3 buckets.
- We actively take precautions to mitigate against Server-Side Request Forgery (SSRF) based attacks that could be used to extract unauthorized data from internal services.

We follow industry best practices for Web Authentication (AuthN) and Access Control (AuthZ) to ensure that users of Remind are only able to access data that they're authorized to access. Records in our data warehouse are separated into PH-containing and non-PH-containing tables. Data in PH-containing tables are deleted after 90 days.

An executed copy of ESBOCES' Parent's Bill of Rights is attached hereto and incorporated herein.