Security and Privacy at Core

Our policies are based on the following foundation principles:

1. Access should be limited to only those with a legitimate business need and granted based on the principle of least privilege.
2. Security controls should be implemented and layered according to the principle of defense-in-depth.
3. Security controls should be applied consistently across all areas of the business.
4. The implementation of controls should be iterative, continuously maturing across the dimensions of improved effectiveness, increased auditability, and decreased friction.

Core maintains a SOC 2 Type II attestation.

Data Protection

Data at Rest

All data stores with customer data are encrypted at rest using AES 256-bit encryption.

Data in Transit

Core uses TLS 1.2 or higher everywhere data is transmitted over potentially insecure networks. We also use features such as HSTS (HTTP Strict Transport Security) to maximize the security of our data in transit.

Enterprise Security

Endpoint Protection

All corporate devices are centrally managed and are equipped with anti-malware protection. Endpoint security alerts are monitored with 24/7/365 coverage. We use MDM software to enforce secure configuration of endpoints, such as disk encryption, screen lock configuration, and software updates.

Security Education

Core provides comprehensive security training to all employees upon onboarding and annually. In addition, all new employees attend a mandatory live onboarding session centered around key security principles. Core's security team shares regular threat briefings with employees to inform them of important security and safety-related updates that require special attention or action.

Identity, Access Management, and Authentication

Core employees are granted access to applications based on their role. Further access must be approved according to the policies set for each application. Strong passwords and multi factor authentication enforced.

Company Policies and Procedures

Core security, risk, and compliance processes were developed based on industry best practices and are reviewed and updated on an annual basis or upon any significant change.

All employees go through training upon hire and must recertify on an annual basis.

Incident Response Planning & Team in place to handle any significant security event to triage and respond to establish system resiliency, minimize impact, and protect customer data.

Regular Third-Party Security Review that identifies and evaluates security risks of vendors and third parties.