Encircle

ENCIRCLE SECURITY QUALIFICATIONS

This document outlines the various processes and systems that Encircle has in place to ensure that customer data is secure. Each organization typically has different security requirements and we encourage you to reach out with any questions as you read through the material.

INCIDENT RESPONSE PLAN

Encircle has a documented Incident Response Plan in place with notifications set to be issued to customers within four hours of any incident.

PERSONNEL TRAINING & CONFIDENTIALITY

Encircle employees with system access are trained and qualified to handle sensitive materials. All employees are under strict confidentiality and conflict of interest agreements.

PRIVACY OFFICER

Mike Kirkup, CTO, acts as Encircle's privacy officer.

CHANGE MANAGEMENT CAPABILITY

Encircle has a robust change management process in place to ensure that only validated software is released from development to staging, and then ultimately to production.

ENTERPRISE ARCHITECTURE

Encircle is committed to best practices for enterprise architecture and the platform that delivers its services is multi-tiered. The server infrastructure is also multi-tiered.

WEB APPLICATION SECURITY ASSESSMENT

Encircle performs an annual external penetration test on its infrastructure (black box approach) through a third party firm. A copy of the most recent report can be provided to any customer who requests it.

Encircle

ENCRYPTION OF USER CREDENTIALS

Encircle protects user credentials using bcrypt, as research shows it is more secure and reliable for generating keys from passwords

STORING AND TRANSMITTING CONFIDENTIAL MATERIAL

All data is encrypted via TLS during transit and encrypted for backups via AES. Data in the database remains in the processing state and would not be encrypted. Encircle also implements the HSTS protocol to ensure strong protection of connections.

CENTRALIZED MONITORING AND LOGGING

Encircle has a centralized monitoring and logging solution in place to manage security information and events. We maintain this log for at least six months to ensure that all actions are effectively logged.

SYSTEM PATCHING AND MAINTENANCE

Encircle uses an n-1 patching approach to ensure patches are regularly performed and maintained to computers developing its software.

PHYSICAL SECURITY OF DATA

Encircle's infrastructure is hosted on the Microsoft Azure platform where only key employees of Microsoft are provided with physical access to the servers. Documentation can be accessed from Microsoft to confirm their processes as necessary.

LOCATION OF DATA CENTERS

Encircle's servers are located in the "Canada Central" zone of Microsoft Azure with our disaster recovery zone being "Canada East." All data stored within Encircle is contained and remains in Canada.