Collective[i] - Security Whitepaper

Security measures we use to protect our clients' data.

Collective[i] Security Team, August 2021

security@collectivei.com

collective[i]®

450 Park Ave South
New York, NY 10016
+1 646.400.5011

Table of Contents

collective[i]®

collective[i]®

450 Park Ave South
New York, NY 10016
+1 646.400.5011

Introduction

The world has changed, data now drives it, and data is Collective[i]'s primary resource. It is also our clients' main asset and, as such, we treat it as if it was our own and protect it with the best of breed controls and processes.

We consider data security and information security as core principles for our business, and we invest in updating and improving our knowledge, controls and processes.

This Security Whitepaper covers the main aspects and principles guiding us in securing our clients' data and the company as a whole.

Standards, frameworks and compliance

Collective[i] follows industry best practices. Our security program follows defence-in-depth principles (layered defense), with controls overlapping one another where applicable, multiple controls covering the same domain, and using controls from different vendors.

We are using NIST frameworks to guide our risk assessments and our security program as a whole.

We follow CSI Top 20 as a guiding principle to deploy our controls and verify their effectiveness. Collective[i] has achieved SOC reports: Type II Soc 2 and 3 since 2018.

450 Park Ave South
New York, NY 10016
+1 646.400.5011

Visit our Trust Center to obtain a copy of the SOC 3 report, or contact our sales team for a copy of the SOC 2 report. Our company and the controls we deploy are being audited annually by a well-known auditing company to achieve SOC accreditation.

Data privacy and security

As data is our primary resource, we protect it carefully. We understand that our clients' data is essential to them, and so is their data privacy and security.

Data is protected in transit using TLS 1.2 and at rest using AES256 encryption. Our employees do not access raw data directly. However, a select group of data scientists may access raw data for maintenance or fine-tuning purposes.

All data in Collective[i]'s network is anonymously contributed, and a client would not be identified to any third party as the source of the data it contributes.

Collective[i] partners with TRUSTe/TrustArc, the leader in privacy compliance and data protection for over two decades, to ensure our clients' data is safe and secure.

Our Privacy Policy is available on our site for further reading.

450 Park Ave South
New York, NY 10016
+1 646.400.5011

Policies and procedures

To ensure security is maintained at all times, Collective[i] publishes internal policies and procedures. These policies are reviewed and updated on an annual basis.

Employees are required to read and follow these policies and are trained on their content on an annual basis.

The main policies in use are:

- Information security policy
- Acceptable use policy
- Privacy and data privacy policy
- Collective[i] code of conduct

Our contractors and vendors are required to follow and adhere to these policies.

Procedures and processes are in place to make sure we address vulnerabilities and incidents promptly.

450 Park Ave South
New York, NY 10016
+1 646.400.5011

The main processes we use are:

- Incident report and response
- Business continuity
- Vulnerability management process
- Risk analysis process

Personnel and training

Collective[i] hires talented people after careful considerations. We screen all candidates and contractors before employment.

Each employee goes through a comprehensive security training program based on their role and receives the following training:

- General security training
- Data and information security awareness training
- Secure code writing (for engineers)

collective[i]®

450 Park Ave South
New York, NY 10016
+1 646.400.5011

Our data centers

Collective[i] uses shared Tier-3 data centers (CoLo). We use two separate data centers located in two different states in the US, with more than 1,000 miles between them.

Our data centers are equipped with the best-of-breed security controls.

- Physical access controls using fences and guarded gates 24/7
- Human monitored security cameras
- Alarms
- Environmental controls (HVAC, Humidity)
- Power outage controls (UPS and generators)

Our data centers are accredited with security certifications

- SOC 2 Type II
- ISO 27001
- NIST 800-53 High

collective[i]®

450 Park Ave South
New York, NY 10016
+1 646.400.5011

Application security

Our engineers develop our platform by following secured code principles. Our development team follows Secure Software Development Lifecycle (SSDLC) based on NIST, NCSC and Microsoft's standards.

Each developer goes through security training on their first day of employment before writing any code for the company. After that, the secured code writing training is repeated on an annual basis.

Our engineers follow best code writing practices such as OWASP's top 10.

An independent third-party penetration tester tests each major product release. As a result, identified vulnerabilities (critical and high) are fixed before each GA release. In addition, medium vulnerabilities and below are addressed in the regular release cadence.

Network security

Our servers within our shared data centers (see above) are segmented to provide high availability and better security.

Our clients' data is fully separated from corporate data.

collective[i]®

450 Park Ave South
New York, NY 10016
+1 646.400.5011

We deploy network security controls to protect the network from unauthorized access or data exfiltration.

- Network firewall (layers 3 and 4) to protect against network-based attacks
- Application firewall (layer 7)
- IDS/IPS with anomaly detection
- SIEM for alerts and logs aggregation

Business continuity

To ensure business continuity, Collective[i] uses Tier-3 data centers (99.995% up-time). Our CoLos are replicas of one another, with data replication mechanisms.

Building on best-of-breed technology, we ensure each data segment is rapidly replicated and has several copies on our systems, thus achieving redundancy on every date layer.

We use periodic backups to ensure our ability to return to a fully operational state if an incident occurs.

450 Park Ave South
New York, NY 10016
+1 646.400.5011

Vulnerability management

We understand that vulnerabilities are inevitable and, as such, we are doing our best to capture them as soon as possible.

We use a centralized managed end-point security platform for all of our devices. Mobile devices are managed with an MDM solution, deploying patches and allowing us remote control (and remote wipe) when needed.

Our servers are monitored 24/7 for vulnerabilities using centralized managed antivirus and host-based IDS (on top of the network IPS).

We encourage our clients to report identified vulnerabilities, and we address each of those reports.

Our application is audited regularly, scanned for vulnerabilities, and frequently undergoes independent penetration tests (see Application security above).

Resources and contact details

- Collective[i]'s Trust Center
- Collective[i]'s Privacy Policy
- For general security questions, please contact the Collective[i]'s Security Team