**Civinc Security Policy**
***Last updated 15/03/2024***

Anonymity and privacy are the cornerstone of the Civinc method, so naturally keeping data of clients and users secure is of high importance to us. We have implemented appropriate technical and organizational measures to ensure that all data that is processed at Civinc is handled in a secure manner.

### 1. Human Resource Security

We ensure that the number of people that have access to systems or information about our Users as well as User Data is limited as much as possible. The only personnel with back-end access to such information currently are director-level employees. Any personnel granted with such access obtains this on a non-disclosure basis. Our staff termination process includes revoking relevant access rights and invalidating all access.

### 2. Data Security

At Civinc we limit as much as possible the personal data we collect based on the legitimate interest of enabling and improving the optimal use of the platform and ensuring the security and stability of the platform, in line with the privacy policy and terms of service.

All data is hosted on the Google Cloud Platform on servers within the EU. All relevant Google Cloud services have successfully completed the ISO 27001 and SOC 1, SOC 2, and SOC 3 evaluation process, and some have also completed the ISO 27017 and ISO 27018 certification process. Google Cloud services encrypt data in transit using HTTPS and logically isolate customer data. The Google Cloud services used by Civinc also encrypt their data at rest. Penetration tests are done by Google Cloud services on their infrastructure on a continuous basis. We have integrated App Check, which helps protect our services by making sure all calls are made by trusted sources. More information op appcheck can be found here. For more information on the security measures taken by relevant Google Cloud services please see here:

- https://firebase.google.com/support/privacy
- https://cloud.google.com/bigquery/docs/data-governance

In order to conduct an AI analysis of relevant sessions on the platform, we use an AI model of OpenAI hosted in the EU by Microsoft Azure. Azure OpenAI doesn't use customer data to (re)train models. For abuse monitoring purposes Azure OpenAI stores all prompts and generated content securely for a maximum of thirty (30) days. More information on data security for Azure Open AI can be found here.

Internally, our technical team ensures security remains a high priority as part of continuous development and improvement efforts, in order to identify and address potential security holes early.

### 3. Incident Response

We have an incident management process to detect and handle Security Incidents which shall be reported directly to the CTO (security@civinc.co) as soon as they are detected. This applies to Civinc employees and all processors that handle personal data. All Security Incidents are documented and evaluated internally and an action plan for each individual incident is made, including mitigatory actions. If you are affected by the Security incident, we will contact you as soon as possible through relevant channels.

## 4. Security Revision Schedule

| Planned Activity | Frequency |
|---|---|
| Revoke system, hardware and document access | End of employment |
| Ensure access levels for all systems and employees are correct | Once per year |
| Ensure all critical system libraries are up to date | Continuously |
| Unit and integration tests to ensure system functionality and security | Continuously |
| External vulnerability scans to ensure system security | Continuously |

## 5. Continuous improvements

Our engineering practices ensure that we have security in mind in all stages of a development lifecycle. While no system is completely secure, we will do our utmost to minimize any type of risk. Examples of Engineering practices:

- Clear code conventions enforced by static code analysis;
- Use of well-known frameworks to protect against common attack vectors (XSS, CSRF, SQL Injection);
- Incident response plans are maintained and followed to quickly act on incidents;
- Continuous check-up to keep libraries up-to-date;
- Continuous integration builds and testing;
- Continuous improvement process with the entire product team where security issues are a standing item;
- Vulnerability scanning is done continuously with use of dedicated third party tooling to ensure the system is protected from any new security threats.
- Penetration tests are done by Google Cloud services (see 2) on their infrastructure
- All releases are tested before merging to production.

## 6. Contact

You can reach Civinc about this Security Policy or any other issue by emailing to security@civinc.co.