IMPACT platform
Data Privacy, Security, and Governance

Updated December 4, 2021

INTRODUCTION

The Central Inspection has put the IMPACT platform at the service of public actors for the collection of various types of data through its platforms (registration for vaccines, sending requests for permits, collecting data on vulnerable households, reporting incidents in hospitals, etc.) in order to enable institutions to properly and safely carry out their functions.

It was therefore crucial from the outset that strict measures be taken in order to ensure the proper handling of data in accordance with Lebanese law and best practices. Privacy protection and security of the data are at the core of the development of the platform. Below is an overview of the privacy and data security measures taken by the Central Inspection.

PRIVACY MEASURES

Privacy policies and terms of use: IMPACT has privacy policies and terms of use specifically tailored for each platform launched on IMPACT. Each privacy policy clearly outlines to the user, *inter alia*, how the data is being handled and by whom. As to the terms of use, they set out, among others, in which manner the platform may be used, and prescribe the prohibited activities.

Data location and backup: Regarding data location, the data is hosted OGERO with a Disaster Recovery also located at OGERO. Data is saved on a backup in the same ecosystem at OGERO and under the same security rules.

Safe Deployment process: Engineers write code and don't have any access to the live severs under any circumstance. The code is pushed to a QA repository for testing and an automated process builds the code then pushes it on the machine where it should be deployed. Any issue that takes place is troubleshooted on the QA and staging environment in order to be reproduced and fixed before live deployment.

Testing: When the code goes through the staging environment, security test (ongoing penetration tests are being conducted before live implementation to ensure that no vulnerabilities exist), unit test, regression test, and load testing are performed.

Team's access denied: Regarding data access, all necessary measures have been taken to ensure only authorized parties have access to personal information. Access to the personal data collected on the various platforms is limited to dedicated staff within indicated entities for the specified purposes in each of the privacy policies through jump server/PAM (Privileged Access Management). Additionally, staff and consultants from Siren have no access to the personal and sensitive information.
A user access review is being executed regularly in order to ensure that all accesses are being granted as per business needs and as per the user access management policy.

Code ownership: All code repositories, code ownership, copyrights & trademarks are registered under Central Inspection and owned by the Lebanese State.

DATA STORAGE AND SECURITY

Protection tools: The technical team has put in place procedures and technologies as per good industry practices and in accordance with applicable laws, to maintain security of all data. As such, protections are set up to prevent **Distributed Denial of Service** (DDoS) attack. The security measures include the setup of a **reCAPTCHA** check upon the submission of the form for the validation of the phone number as well as an **automatic IP blocking** of addresses identified through intrusion prevention systems as constituting a potential security risk.

All communication between a user's computer and the servers is established over **SSL connections** using CA-issued certificates, and no intermediary CDNs (Content Delivery Network). **Protection measures** are embedded against system, network, and application attacks (OWASP Top 10 2021-2017, ISO27001, CIS, ASVS best practices, etc.) through:

- Security by design Secure SDLC
- WAF/IPS with SSL offloading
- EDR and NDR

Additionally, should the data be physically attacked, the disks used by the operating system hosting the platforms are **encrypted using LUKS2** which is decrypted manually when the system starts up **with a passphrase** available to select individuals within Central Inspection. Performing a brute force attack against a passphrase which can be of 20 characters for example would require 82^{20} combinations which is practically impossible to uncover, even in years.

Crisis Management: A 2-factor authentication system is set in place, limiting such access to the servers to individuals who have been granted access explicitly and after justification. A temporary code/token is generated by the President of Central Inspection to provide server access to the selected developers to troubleshoot issues. The system shall be managed by dedicated staff within Central Inspection supported by two senior Siren Engineers.

A PAM (Privileged Access Management) and Firewall have been installed with a password shared between OGERO, PCM and Central Inspection. This security measure allows organizations to control and monitor the activity of privileged users down to the keystroke without being able to turn it off.

Security review and penetration testing: POTECH, a Lebanese well known security firm has been hired to regularly audit the system and oversee its security standards. POTECH has been working closely for several months with the team to execute internal and external security audits, produce penetration + compromise testing on the system and provide regular reports. Potech has been interacting with the team daily, producing weekly feedback and monthly reports since January 2021.

Below are the executed tasks:

- Black box/grey box APIs penetration test
- Grey box external web application penetration test
- Internal penetration test
- Cyber threat intelligence report and digital risk protection
- Compromise assessment
- High level IT architecture review

Below are the ongoing tasks:

- Retests on the web applications and APIs
- Technical security assessment on the available systems and databases
- User account review

- Regular IT infrastructure security assessment (review the configuration of all security and network equipment such as firewall, EDR, etc.)
- IPS fine tuning

Policies and measures: POTECH has also assisted the Team to develop and enforce written policies for:

- Information Security Incident Management
- User Access Management
- Backup and Restore Management
- Change management
- Password splitting
- Information security charter listing all roles and responsibilities of all entities.

Team NDAs: All Siren team members have signed an NDA with the Central Inspection and undertaken a security training to develop secure code by design. The Siren team's names, IDs and full information were shared with the Lebanese Army's intelligence department from the very inception of the project (in May of 2020) for security review.