**Requirement:**

Projects collecting data must identify the types of data collected and stored. Projects must also demonstrate how they ensure the privacy and security of this data in addition to the steps taken to prevent adverse impacts resulting from its collection, storage, and distribution.

**Approach taken for development of DiCRA:**

The platform uses and generates data analysis on natural resources impacting agriculture (soil, water, land, meteorological conditions etc.), wealth index (of geographies) and markets (price fluctuations of agriculture commodities). Majority of the data sets used and generated by the platform are non-PI in nature that are transparently available to the highest possible disaggregated levels through the DiCRA platform.

The only PI data captured by the platform is basic information of users who extract data from the platform through simple download or through Open APIs. Minimal PI information such as user name and email ID are the only details captured by the platform. This information is collected to understand user engagement on the platform and for communicating updates on the platform. User statistics – like downloads, API calls, traffic etc., are aggregated and transparently available on DiCRA platform.

The PI data, however minimal, is stored on UNDP’s cloud infrastructure and secured through multifactor authentication system. There are strictly no ‘third party’ data transfers of the PI data through this platform.

The application vulnerabilities are handled through Open Web Application Security Project (OWASP) application security verification standards. This ruleset protects our application from common threats defined in the top-ten OWASP categories. A pre-configured rule set is managed by the Azure WAF service is enabled to protect from common threats as described in the screenshot below.

Graphical user interface, table

Description automatically generated

The application vulnerabilities are handled through Open Web Application Security Project (OWASP) application security verification standards. In order to make the application secure, the following security risks are being taken care of:

* Broken Access Control
* SQL Injection
* Insecure Design
* Security Misconfiguration
* Cross-Site scripting

UNDP has done User Acceptance Testing for the application.