TCRC Web Application Development Standards

1. **Web Application Development Tech Stack Standards**:

   To ensure consistency, maintainability, and security in web application development, TCRC enforces the following technology stack requirements for all internal projects and those outsourced to external developers:

   1.1. **Framework**: All web applications developed by TCRC or outsourced to external developers must use the **Laravel framework**. This ensures compliance with TCRC's technology stack policy and aligns with TCRC's in-house support capabilities.

   1.2. **Frontend Solutions:** Developers are encouraged to use the **Laravel Blade** templating engine for front-end solutions. Additionally, developers may leverage popular front-end scaffolding tools like **Vue.js, Bootstrap,** and **React** as needed to enhance user experience and interface functionality.

   1.3. **Database Standard: MySQL** must be utilized as the database for all applications. This standard ensures uniformity in database management and ease of maintenance across TCRC projects, facilitating better support and collaboration.

2. **Standard Web Application Development Procedures**:

   To maintain a consistent development workflow, developers must adhere to the following procedures throughout the project lifecycle:

   2.1. **Source Code Management**: From the inception of the project, all source code must be version-controlled and stored within the *TCRC GitHub Organization*. This applies to both in-house developers and external freelance developers or companies. The repository must be updated continuously, reflecting every significant change in the project.

   2.2. **Development Best Practices**: Developers must follow the best practices for Laravel development, especially concerning *backend module development* and *API creation*. These practices are curated and maintained by TCRC's internal development and security teams. The latest version of these best practices is made available on TCRC's *GitHub documentation* and will be regularly reviewed and updated.

   2.3. **Architecture Design Documentation**: Before initiating development, developers must create and submit a comprehensive *Architecture Design Document*. This document should be based on the agreed requirements and discussions with both the client and TCRC's technical team. It must cover the entire system architecture, flow, modules, and interactions between components. Development work may only proceed once this document has been reviewed and approved.

   2.4. **Code and Functional Documentation**: Developers are responsible for maintaining clear, up to date *code documentation* throughout the development process. This

includes documenting all modules, key functions, and API interactions. Additionally, the functionality of each module must be thoroughly documented to ensure ease of future maintenance.

2.5. **Code Audits and Rectifications**: Developers must comply with the recommendations outlined in *code audit reports*. These audits will be conducted post-testing to identify any security vulnerabilities, coding inefficiencies, or deviations from best practices. It is the developer's responsibility to address these issues before deployment.

3. **Web Application Deployment Standards**:

To ensure portability, security, and long-term maintainability, TCRC has established the following deployment standards for all web applications:

3.1. **Containerization**: All applications and their associated databases must be deployed using *Docker*. This ensures that the applications can run consistently across different platforms and environments, minimizing deployment and scaling challenges.

3.2. **Security Best Practices**: All deployments must strictly adhere to the *security best practices* established by TCRC. These guidelines assist in marking all the checkboxes to ensure secure deployment of application on server. These security best practices are regularly reviewed and updated by TCRC and are available on the *TCRC GitHub* repository for developers to consult.

By adhering to these standards, TCRC ensures that all web applications are developed and maintained in a uniform, secure, and scalable manner. All developers, both in-house and outsourced, are required to comply with these standards to ensure high-quality deliverables and effective long-term maintenance. Non-compliance with these guidelines may result in the action outlined in the TCRC Non-Compliance Policy for Web Application Development Standards.