BUSYBEE
info@mybusybee.net
www.mybusybee.net
(02) 8929-2222 / (02) 8374-9146 / 09178372000
G7 Burgundy Place 8. Gonzales St. Loyola Heights, Quezon City. Ph 1108

SUBJECT **INSTALLATION AND DEPLOYMENT PLAN FOR THE PRIMARY CARE WORKERS CERTIFICATION ONLINE SYSTEM (PCWCOS)**

Dear Sir/Ma'am,

Good day.

This letter provides the **updated step-by-step installation plan** for the deployment of the **Primary Care Workers Certification Online System (PCWCOS)**, including the reconfiguration of the system server to ensure optimal performance, security, and reliability.

Step 1: Pre-Deployment Preparation
All existing system data and configurations will be backed up. A readiness check will be conducted to verify server capacity, network connectivity, and required software dependencies. Roles and responsibilities of the deployment team will also be confirmed.

Step 2: Server Reconfiguration
The system server will be reconfigured by updating the operating system, applying necessary patches, and optimizing CPU, memory, and storage allocation. Security hardening will be implemented by configuring firewalls, restricting access, and disabling unused services. Backup and monitoring tools will also be set up.

Step 3: Environment Setup
Required system software such as the web server, database management system, and application runtime environment will be installed and configured to support PCWCOS.

Step 4: Database Installation and Configuration
The database will be created and configured, including the setup of schemas and user access. Initial or existing data will be imported and verified for accuracy and integrity.

Step 5: Application Installation
The PCWCOS application will be deployed to the server. Configuration files and environment variables will be set, and appropriate file permissions will be applied to ensure proper system operation.

Step 6: System Integration
Necessary integrations such as user authentication services and notification systems (e.g., email or SMS) will be configured and tested.

Step 7: Testing and Validation

The system will undergo comprehensive testing to ensure all components are functioning correctly and meet operational requirements. This includes functional testing, performance testing, and user acceptance testing (UAT).

Specific validation will cover the following key functionalities:

- **Form Submission:** Ensure all required fields, input validations, and error messages are functioning correctly. Verify that submitted data is accurately stored and retrievable, and that confirmation messages are displayed after successful submission.
- **Update Password:** Validate current password verification, enforce password complexity requirements, and confirm successful password updates. Ensure proper error handling for incorrect or mismatched inputs and verify that users can log in using the updated credentials.
- **Email Notifications:** Test the sending of system-generated emails such as registration confirmations, password reset notifications, and submission acknowledgments. Ensure emails are delivered to the correct recipients, contain accurate information, and are properly formatted.

In addition, prior to production deployment:

- All **displayed One-Time Passwords (OTP)** within the system interface must be removed to ensure security.
- All **test accounts and dummy data** used during development and testing must be deleted to prevent unauthorized access and maintain data integrity.

Step 8: Security Implementation

Security measures including SSL/HTTPS configuration, role-based access control, and data protection mechanisms will be enforced. System logs and audit trails will also be activated.

Step 9: Deployment (Go-Live)

The system will be deployed to the production environment during a scheduled maintenance window to minimize disruption. Final checks will be conducted prior to granting user access.

Step 10: Post-Deployment Activities

After deployment, the system will be continuously monitored to ensure stability,

performance, and availability. Immediate issues or bugs will be addressed, and user support and initial training will be provided.

Step 11: Vulnerability Assessment and Penetration Testing (VAPT)

A comprehensive VAPT will be conducted to identify and assess security vulnerabilities within the system. If issues or vulnerabilities are identified in the results, the development team will perform necessary remediation by fixing the source code and system configurations. The system will then undergo retesting and repeated VAPT cycles until all identified vulnerabilities are resolved and the system meets required security standards.

Additionally, any **false positives** detected during the VAPT must be carefully **identified, documented, and reported to the DOH Knowledge Management and Information Technology Services (KMITS)** team to ensure transparency, proper assessment, and appropriate follow-up action.

Step 12: Pre-Deployment for Enhancements/Updates
Following VAPT and initial deployment, any required system enhancements, patches, or updates will undergo a pre-deployment process in a staging environment. This ensures that improvements are tested and validated before being applied to the live system.

This structured approach ensures a smooth, secure, and efficient deployment of the PCWCOS. We respectfully seek your approval to proceed with the implementation.

Thank you.

FRANZ DARYL DUETES
PROJECT MANAGER
MyBusyBee, Inc.