# System Installation Plan

This document outlines the plan for installing the Licensing Self-Certification Portal (LSCP) system for the Buildings Department (BD). It covers the project environment, deployment procedures, and installation schedule.

## 1. Introduction

This System Installation Plan describes the procedure and schedule for deploying the LSCP application in the production environment. The system comprises three main parts:

* Database Server
* Backend Server
* Frontend and Web Portal Server

## 2. Project Environment Description

### 2.1 Network Diagram

The production and UAT sites are located in 1/F West Kowloon Government Office.

[DIAGRAM HERE]

The network is separated into three zones: DMZ, trusted zone, and storage network. A two-tier firewall setup is used to form the trusted zone and DMZ. Incoming network traffic must pass through the DMZ before entering the trusted zone.

To optimize hardware resource utilization, most servers (except the backup server) are virtual machines (VMs) consolidated into DMZ and trusted zone VM host servers. Two VM host servers are built in each zone for high availability.

Storage is consolidated and provided by SAN storage with a dedicated network interconnected with the VM host servers. The backup server resides in this storage-dedicated network for backup tasks of VM host servers in both DMZ and trusted zones.

### 2.2 Hardware Specification

#### Production and UAT Environment

List of machines and virtual machines:

| Hostname (Physical Machine) | Hostname (Virtual Machine) | Purpose | IP |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

#### DR Environment

List of machines and virtual machines:

| Hostname (Physical Machine) | Hostname (Virtual Machine) | Purpose | IP |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### 2.3 Software Specification

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 3. Application Deployment Procedure for Production

### 3.1 Database Server

To install the database server:

1. Remote login to PRD-DB-01(10.5.113.218).

### 3.2 Backend Servers

1. Remote login into PRD-WEBAPP-01.

### 3.3 Frontend Servers

1. Remote login into PRD-WEBAPP-01.

#### 3.3.1 sFTP Server Setup

1. Install OpenSSH server in Windows Server. Go to Apps & Features, click ?Optional Features?, click ?Add a feature?, check ?OpenSSH Server?.

## 4. System Installation Schedule and Result

### 4.1 System Installation Schedule

The following table summarizes the testing schedule:

| Pre-Requisite |  | Start Date | End Date | Start time | End Time |
| --- | --- | --- | --- | --- | --- |
| Database Server Installation (Production and DR) |  |  |  |  |  |
| Backend Server Installation (Production and DR) |  |  |  |  |  |
| Frontend Server Installation (Production and DR) |  |  |  |  |  |
| Functionality test (VM & Networking) |  |  |  |  |  |
| Database setup |  |  |  |  |  |
| Deployment for 1st version of frontend server |  |  |  |  |  |
| Deployment for 1st version of backend server |  |  |  |  |  |
| Application Health Check |  |  |  |  |  |
| 1 |  |  |  |  |  |
| Deployment for Latest Mobile Application |  |  |  |  |  |
| Final Check Production Web Server |  |  |  |  |  |
| Final Check Production Database Server |  |  |  |  |  |
| Final Check DR Web & Database server |  |  |  |  |  |
| Final Check IIS & Framework |  |  |  |  |  |

### 4.2 System Installation Result

The following table summarizes the actual system installation schedule:

| Pre-Requisite |  | Actual Start Date | Actual End Date | Actual Start time | Actual End Time | Status/Result |
| --- | --- | --- | --- | --- | --- | --- |
| Database Server Installation (Production, UAT and DR) |  |  |  |  |  |  |
| Backend Server Installation (Production, UAT and DR) |  |  |  |  |  |  |
| Frontend Server Installation (Production, UAT and DR) |  |  |  |  |  |  |
| Functionality test (VM & Networking) |  |  |  |  |  |  |
| Database setup |  |  |  |  |  |  |
| Deployment for 1st version of frontend server |  |  |  |  |  |  |
| Deployment for 1st version of backend server |  |  |  |  |  |  |
| Application Health Check |  |  |  |  |  |  |
| 1 |  |  |  |  |  |  |
| Deployment for Latest Mobile Application |  |  |  |  |  |  |
| Final Check Production Web Server |  |  |  |  |  |  |
| Final Check Production Database Server |  |  |  |  |  |  |
| Final Check DR Web & DB server |  |  |  |  |  |  |
| Final Check IIS & Framework |  |  |  |  |  |  |

## Appendix: System Manual Information (Summary)

This section summarizes key information from the System Manual relevant to installation and configuration.

### 5. System Summary

* **5.1 Objective:** Provide an electronic platform for site inspection and monitoring personnel to manage inspection records.
* **5.2 System Architecture:** The LSCP operates across two data centers: On-premise (WKGO) and Government Cloud Infrastructure Services (GCIS). The architecture includes firewalls, reverse proxy servers, web application firewalls (WAFs), application servers, web servers, and database servers. Key components include:
  + External Application Server (IIS, React framework)
  + External Web Server (IIS, ExpressJS)
  + BD Web Servers (Internal BD users)
  + Database Management Servers (Microsoft SQL Server)
  + Web Browser Support (See image in original document)
  + Integration with iAM Smart, Departmental Portal, SMTPX, MWMS, and BCIS.

### 6. Equipment Configuration

This section details the hardware and software configurations for Production, DR, UAT and DEV environments. Refer to the original System Manual for detailed tables on:

* **6.1 Computer Hardware:**
  + Hardware Components (Physical Servers, SAN Storage, Backup Storage, Tape Library, Firewalls, Switches, KVM, UPS) in Production and DR sites.
  + Partition Configuration of Production and DR Servers.
* **6.1.2 Guest Servers Components:**
  + Production, UAT, DEV and DR guest servers (Role, Host Name, vCPU, RAM, Disk, IP Addresses, Data Center, Host Server/Zone).
* **6.1.3 Gateway and SMTPX Configuration:**
  + SMTPX configuration details (service hostname, IP addresses, port number, authentication).
  + WKGO Production Network Gateway and AIA DR Network Gateway details (Gateway, Subnet, IP Range, vlan/Zone).
* **6.1.4 Database Configuration:**
  + Database server details for WKGO Production, UAT, DEV, AIA DR, GCIS P1, GCIS UAT, GCIS DEV, and GCIS P2 DR.
* **6.1.5 Detailed Server and Network Configurations:**
  + Rack diagram (See image in original document).
  + External and Internal Firewall configurations (reference to other documents).
  + Windows NLB configuration (reference to other documents).
  + Switches - Prod DMZ Port, Prod INT SW Port, DR DMZ SW Port, DR INT SW Port (See images in original document).

### 7. Software Inventories

This section lists the software installed on each server. Refer to the original System Manual for detailed tables on:

* **7.1 Inventory of Application Programs:** Details in Program Manual (T352).
* **7.2 Inventory of System Software and Software Package:**
  + Production Environment ? WKGO
  + UAT Environment ? WKGO
  + DEV Environment ? WKGO
  + Production Environment ? GCIS P1
  + UAT Environment ? GCIS T1
  + DEV Environment ? GCIS T1
  + DR Environment ? AIA
  + Production Environment (Replicate from P1) ? GCIS P2
  + Frameworks Used During Development (React, ExpressJS, NodeJS)

### 8. Security and Backup

* **8.1 System Control:** Authentication via OSDP for BD staff; OTP via email for external users. Password complexity follows IT Security Guidelines.
* **8.2 Backup:**
  + WKGO and AIA: Daily VM image backup to backup storage, weekly to tape, daily copy to AIA. Database servers perform local backups.
  + GCIS P1: Backup services provided by GCIS with offsite copy and replication to DR GCIS P2. Database server performs local backup.
  + UAT and DEV (GCIS): Backup services provided by GCIS.
* **8.3 Security:**
  + Data Transmission Security: HTTPS over TLS.
  + Data Storage and Auditing Security: SAN storage in production, local server storage in DR. RAID mirroring, data encryption, audit trails.
  + System Security: Regular service pack and patch updates. Antivirus clients managed by a virtualized Antivirus Management server.
  + Physical Security: Server rooms compliant with IT Security Guidelines.
  + Password and Group Control: Password control, DP login for BD users, OTP for internet access, iAM Smart app login. User access limited by user group assignment.
  + Control Procedure of Application User Account and Production Support Account: Registration process, vetting by Head of Stream. Application Maintenance Team access to production servers requires System Maintenance Committee approval.
* **8.4 Change Control:** Program source maintained by the Application Maintenance Team with GIT repository.
* **8.5 Disaster Recovery:**
  + GCIS: Automatic failover to GCIS Prod 2. Daily database backup.
  + BDSCS External (On-Prem): Load balancing with NGINX. Scheduled database backup. VM replication to DR environment.
* **8.6 Database Backup Strategy:**
  + SQL Database Backup: Full export backup daily.
  + Recovery: Table detailing impact, system recovery, and downtime for various failure scenarios.
  + Backup Schedule: Table detailing backup schedules.

### 9. Database Administration

* **9.1 Clean Database Transaction Logs:** Step-by-step instructions for cleaning transaction logs.
* **9.2 Database Backup:** Step-by-step instructions for performing database backups.
* **9.3 System Constraints and Limitations:**
  + URL path length limit: 250
  + Restricted characters for files/folders: ~, #, %, &, \*, {, }, \ :, <, >, ?, /, |, ?
* **10. Log Management**
  + The following activities shall include in the log: Attempts for log-in, Unauthorised update/access, Failed attempts for privileges elevation, Attempts for password changes, Access attempts to critical files, Actions taken by privileged users, Use of privileged rights such as addition and deletion of user accounts, Security related system failures and alerts, Changes to user access rights, Failed access attempts to systems and files identified as critical to the system, Computer services such as file copying or searching, Modification to audit policy, Activation and de-activation of protection systems, such as anti-malware systems and intrusion detection systems
  + Logs shall be retained for **180 days** and centralised and managed by Syslog server. Unauthorised access is restricted.

## Appendix: User Requirements Specification (URS) - Key Points

This section summarizes key aspects of the User Requirements Specification (URS) document.

### 1. User Requirements

* **1.1 Proposed System Overview:** The LSCP aims to streamline the application process for certificates and notices related to Educational Premises (EP) and Child Care Centers (CCC). It also provides building safety comments to the Education Bureau.
* **1.1.2 System User Profile:** Defines responsibilities and roles for various users, including Applicants, AP/RSE, EDB/SWD Users, Registry, SE, SSE, SO, BS, TO, SBS, CBS, System Admin, and User Admin.
* **1.2 Future Business Process:** Lists and describes future business processes, including:
  + Application for e-Certificates and e-Notice for EP (e-application)
  + Application for Alteration for EP/CCC (e-application)
  + Application for Certificates and Notice for EP (paper application)
  + Application for Alteration for EP/CCC (paper application)
  + Random Audit Check
  + Application for Approval for use of the premises for conducting course under the Non-Local-Higher and Professional Education (Regulation) Ordinance [NLHP(R)O] (e-application)
  + Application for Approval for use of the premises for conducting course under the Non-Local-Higher and Professional Education (Regulation) Ordinance [NLHP(R)O] (paper application)
  + Application for Periodic Inspection for CCC
  + Application for inclusion of Temporary Structures in the Pre-accepted Temporary Structure (PTS) Register for user under TPPE license
* **1.3 Functional Requirements:** Lists detailed functional requirements, categorized as:
  + General Requirement (REQ-GR)
  + Workflow Requirement (REQ-WR)
  + Form Requirement (REQ-FRM)
  + Form Processing Requirement (REQ-PRO)
* **1.4 Non-Functional Requirements:** Lists non-functional requirements, categorized as:
  + Communication Requirement (REQ-CR)
  + Webpage Requirement (REQ-UR)
  + Security Requirement (REQ-SR)
  + Interface Requirement (REQ-IR)
* **1.5 Technical Requirements:** Lists technical requirements (REQ-TR), including:
  + 24x7 Internet and Intranet
  + Integrated Cloud GCIS and On Premises
  + Input Validation
  + Record Relocation from GCIS to On Premises
  + High Availability
  + Monitoring and Alert Generation
  + DR Drill
  + UTF-8, Unicode or HKSCS
  + System Logging
  + High Configurable
  + Backup and Recovery
  + Operation System and Browser Compatibility
  + Review and Update Privilege
  + Health Check
  + Encryption on All Communications
  + Version Control for application
  + Monthly Usage Statistics and Ad-hoc Statistics
  + Check-in and Check-out
  + Language support (EN/TC/SC)
  + System Performance
  + Reports and statistics for monitor system performance
  + Ad-hoc and periodic updates on the contents
  + Provide refined Login & Authentication / FULL Audit features
  + Login user account login by user ID & password
  + Version control of source code
  + System log tracking
  + Scalable system frame design
  + Data exchange with other system securely
  + Security measurement
  + Help check email notification
  + Email notification for all batch jobs
  + Conform to the Interoperability Framework
  + Manage System Parameters
  + Allow System Access by EDB and SWD
  + Independent System (Not depended on other BD system)
  + Logout automatically for inactive for 30 minutes
  + Centralized log management
  + Handle around 300 user accounts of EDB and SWD for single sign on
  + Paper Less
  + PDF template and mapping field for letter generation

### 2. Constraints List

* **2.1 Complexity of Address Identification:** Case creation may be passed to BCIS.
* **2.2 Signature of AP/RSE:** Hand writing signature needs to be verified by Registry using eyeball for paper applications.

### Appendix

* Appendix 1 ? 3-Tier BSR System
* Appendix 2 ? Sample of School and CCC Certificates and Notices
* Appendix 3 ? Sample of Letter of Requirement (LoR)
* Appendix 4 ?Information Security Requirement
* Appendix 5 ?Sample of Utilisation Report