# System Test Plan and Result

## 1. Purpose

This document provides an overview of the system, listing the programs, data files, equipment, clerical procedures, and computer operation procedures. It serves as a guide for staff maintaining the application system.

## 2. Scope

This document outlines the software and hardware configurations for the Licensing Self-Certification Portal (LSCP), including application configurations, server and workstation information, and backup services. It is intended for staff responsible for maintaining the application system.

## 3. References

* Training Manual
* Data Manual
* Program Manual
* Application Operation Manual
* Computer Operation Procedure Manual

## 4. Definitions and Conventions

### 4.1 Definitions

None specified in the provided documents.

### 4.2 Conventions

The following acronyms are used:

* BD: Buildings Department
* LSCP: Licensing Self-Certification Portal
* DMZ: Demilitarized Zone
* SAN: Storage Area Network
* VM: Virtual Machine
* ITU: Information Technology Unit
* WKGO: West Kowloon Government Offices

## 5. System Summary

### 5.1 Objective

The LSCP aims to provide an electronic platform for site inspection and monitoring personnel to manage inspection records. It also enables public users (applicants, Authorized Persons (AP), Registered Structure Engineers (RSE)) and users in Social Welfare Department (SWD) and Education Bureau (EDB) to submit application forms and electronic documents online.

### 5.2 System Architecture

The system architecture involves both on-premise (WKGO) and Government Cloud Infrastructure Services (GCIS) data centers.

* **On-Premise (WKGO):** Behind an internal firewall with NAT, separated into Production, UAT, and DEV environments for internal users. A reverse proxy server with load balancing is used for security.
* **GCIS:** Divided into Internet DMZ (iDMZ), Trusted Zone, and Gnet DMZ (gDMZ). External users access the system through the internet via LSCP Web Application, which interacts with the Application Server through a reverse proxy. The Application Server hosts static web interface files.

The architecture includes various servers for specific functions:

* External Application Server
* External Web Server
* BD Web Servers
* Database Management Servers
* Log Server
* File Server
* vCenter Server
* Backup Server

### 5.3 System Functions

The system functions include:

* Public User Authentication (Password & iAM Smart)
* GEO and BD User Authentication
* User Account Management
* Task Assignment and Notification
* Document Management (Preview, Print, Upload)
* Management Statistics and Reports
* e-Submission, e-Processing, and e-Tracking
* Centralized Data Repository
* Search and Capture
* Handling New and Alteration Applications
* Handling Self-Certification Submissions
* Handling Periodic Inspection for CCC
* Handling PTS for TPPE
* Issue Acknowledgement Letter

## 6. Equipment Configuration

### 6.1 Computer Hardware

Detailed hardware configurations for Production, UAT, DEV, and DR sites are provided, including:

* Server models, hostnames, IP addresses, serial numbers, and disk configurations.
* SAN storage details (type, model, serial number, disk count, IP addresses).
* Backup storage details (type, model, serial number, volume size, IP address).
* Firewall configurations (hostnames, IP addresses, model, serial number).
* Switch configurations (hostnames, IP addresses, model, serial number).
* KVM and UPS details.

Detailed hardware components of production and disaster recovery servers are also listed, including CPU, RAM, HDD, and operating system.

Partition configurations for Production servers are specified.

## 7. Software Inventories

### 7.1 Inventory of Application Programs

Refer to the Program Manual (T352) for details.

### 7.2 Inventory of System Software and Software Package

The following table summarizes the system software and software packages installed on the servers:

**WKGO Production Environment**

* **NAS:** Details not provided.
* **Veeam Backup Server:** Windows Server 2022 21H2, VMware Tools, ESET Server Security, ESET Management Agent, Veeam Backup & Replication.
* **Kiwi Log Server:** Windows Server 2022 21H2, VMware Tools, ESET Server Security, ESET Management Agent, Kiwi Syslog Server NG.
* **NOD32 Anti-Virus Server:** Windows Server 2022 21H2, VMware Tools, ESET Server Security, ESET Management Agent, ESET PROTECT Server.
* **API Server:** Windows Server 2022 21H2, VMware Tools, ESET Server Security, ESET Management Agent.
* **Frontend Server:** Windows Server 2022 21H2, VMware Tools, ESET Server Security, ESET Management Agent, IIS.
* **Backend Server:** Windows Server 2022 21H2, VMware Tools, ESET Server Security, ESET Management Agent.
* **Database Server:** Windows Server 2022 21H2, VMware Tools, ESET Server Security, ESET Management Agent, Microsoft SQL Server 2022, Microsoft Management Studio.
* **File Server:** Windows Server 2022 21H2, VMware Tools, ESET Server Security, ESET Management Agent.
* **Reverse Proxy Server:** Windows Server 2022 21H2, VMware Tools, ESET Server Security, ESET Management Agent, Nginx.
* **vCenter:** vCenter 8.0.3.
* **VM Host:** VMWare vSphere 8.0.3.

**UAT Environment - WKGO:**

* API Server, Frontend Server, Backend Server, Database Server, File Server, Reverse Proxy Server: Windows Server 2022 21H2, VMware Tools, ESET Server Security, ESET Management Agent, IIS (Frontend Server), Microsoft SQL Server 2022 (Database Server), Nginx (Reverse Proxy Server).

**DEV Environment - WKGO:**

* API Server, Frontend Server, Backend Server, Database Server, File Server, Reverse Proxy Server: Windows Server 2022 21H2, VMware Tools, ESET Server Security, ESET Management Agent, IIS (Frontend Server), Microsoft SQL Server 2022 (Database Server), Nginx (Reverse Proxy Server).

**Production Environment ? GCIS P1**

* Veeam Backup Server, Kiwi Log Server, Reverse Proxy Server, Application Server, Database Server: Windows Server 2019 1809, VMware Tools, Bitdefender Endpoint Security Tools, Veeam Backup & Replication (Veeam Backup Server), Kiwi Syslog Server (Kiwi Log Server), Nginx (Reverse Proxy Server), IIS (Application Server), Microsoft SQL Server 2022 (Database Server), Microsoft Management Studio (Database Server).

**UAT Environment ? GCIS T1**

* Reverse Proxy Server, Application Server, Database Server: Windows Server 2019 1809, VMware Tools, Bitdefender Endpoint Security Tools, Nginx (Reverse Proxy Server), IIS (Application Server), Microsoft SQL Server 2022 (Database Server), Microsoft Management Studio (Database Server).

## 8. Security and Backup

### 8.1 System Control

* BD staff authentication via OSDP or username/password + OTP.
* External users authenticated by OTP via email or iAM Smart.
* Password complexity and policy following IT Security Guidelines.
* Function access rights based on user roles.

### 8.2 Backup

* Daily VM image backup stored in backup storage.
* Weekly backup to tape and daily copy to AIA (for WKGO).
* Database servers perform local database backup, copied to AIA.
* GCIS backups provided by GCIS with offsite copy and replication to DR GCIS P2.

### 8.3 Security

#### 8.3.1 Data Transmission Security

Data transmitted over the network is encrypted using HTTPS over TLS. Certificates are applied for web servers, including OGCIO's ISCCA certificate for internal servers and public SSL certificates from HK Post for public-facing servers.

#### 8.3.2 Data Storage and Auditing Security

Data is stored in SAN storage (WKGO) or local server storage (DR). RAID mirroring and encryption are used. Audit trails record add/change/delete actions.

#### 8.3.3 System Security

Regular service pack and patch updates are performed. All servers are installed with antivirus clients managed by a virtualized Antivirus Management server.

#### 8.3.4 Physical Security

Servers and equipment are located in secure server rooms.

#### 8.3.5 Password and Group Control

The LSCP is protected by password control, BD user is able to login via DP of the Buildings Department and Internet, if login via Internet, it requires to submit password plus a one- time password by Authenticator, otherwise only one password requires. Public user can login via Internet and iAM Smart app, login via Internet requires password plus a one-time password by email, login via iAM Smart app requires no password.

User are limited to access specific function, field, case and administrative authority by assignment of user group to user account.

#### 8.3.6 Control Procedure of Application User Account and Production Support Account

* New users register with HKID and AP/RSE registration number verification.
* One-Time-Password (OTP) token for secure login.
* Information vetted by Head of Stream staff.
* Application Maintenance Team access to production servers requires System Maintenance Committee approval and ITU monitoring.

### 8.4 Change Control

Program source code is maintained using GIT repository with version control.

### 8.5 Disaster Recovery

* **GCIS:** Automatic failover to GCIS Prod 2 in case of Prod 1 failure. Daily overnight virtual machine backups retained for 30 days.
* **BDSCS External (On-Prem):** NGINX load balancing across two servers. Daily database export backup to local hard disk, then transferred to AIA.
* VM Replication to DR Environment: All production virtual machines will be replicated to the disaster recovery (DR) environment using the VEEAM architecture, ensuring continuity in the event of a failure

### 8.6 Database Backup Strategy

#### 8.6.1 SQL Database Backup

Database full export backup carried out daily at 18:45.

#### 8.6.2 Recovery

| # | Failure Scenario | Impact