# Computer Operation Procedures Manual

## 1. Purpose

This Computer Operation Procedures Manual (COPM) provides information and operating instructions related to the operation of the Licensing Self-Certification Portal (LSCP) computer system within the Buildings Department (BD). It is intended for use by the operating staff of the relevant sections. This manual supplements, but does not replace, formal technical documentation from manufacturers.

## 2. Scope

This document serves as a guide for operating the LSCP system. It outlines tasks that administrators need to monitor to ensure proper system functionality.

## 3. References

* System Installation Plan
* Application Operation Manual

## 4. Definitions and Conventions

### 4.1 Definitions

None provided in the input 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
* **AIA:** Building Department office at AIA tower
* **ISCCA:** Intranet Server Certificate Certification Authority

## 5. System Summary

### 5.1 Objective

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

### 5.2 System Architecture

The LSCP system architecture includes both an On-premise (WKGO) and a Government Cloud Infrastructure Services (GCIS) deployment.

**On-Premise (WKGO):**

* Internal firewall with NAT separating Production, UAT, and DEV subnets.
* Reverse proxy server with load balancing.

**GCIS:**

* Internet DMZ (iDMZ) and Gnet DMZ (gDMZ).
* Reverse proxy server and Web Application Firewall (WAF) in front of iDMZ.

**Data Flow:**

1. External users access the system via the internet through the LSCP Web Application.
2. The Web Application interacts with the Application Server through the reverse proxy.
3. The Application Server hosts static web interface files.
4. Requests are passed to Web Servers in the Trusted Zone for system logic.
5. Web servers, written in NodeJS, perform CRUD operations on Database Servers (Microsoft SQL Servers) and the in-built file storage.
6. Results are returned to the External Web Servers and then to the internet.
7. Internal users access the system through the Departmental Portal (OSDP) to the BD Web Servers in the Trusted Zone.

**System Components:**

* **External Application Server:** Serves static web content (HTML, CSS, JavaScript) and proxies backend APIs.
* **External Web Server:** Hosts the backend API (ExpressJS) for business logic and database operations.
* **BD Web Servers:** Identical to External Application Server but deployed in internal zones.
* **Database Management Servers:** Microsoft SQL Server database engine.

### 5.3 System Functions

The system provides the following functions:

* UF-WEB-001-1: Public User Authentication with Password
* UF-WEB-001-2: Logout system to clear user session
* UF-WEB-001-3: Single User Session
* UF-WEB-001-4: GEO and BD User Authentication
* UF-WEB-001-5: Public User Authentication with iAM Smart
* UF-WEB-001-6: Forgot Password
* UF-WEB-001-7: Change Password
* UF-WEB-001-8: Public Users create/register an account
* UF-WEB-001-9: User Account Confirmation
* UF-WEB-001-10: Resend User Account Confirmation Email
* UF-WEB-001-11: User Account Detail Management
* UF-WEB-001-12: User Email Address Update Confirmation
* UF-WEB-001-13: Public User Accounts Management
* UF-WEB-001-14: BD User Accounts Management
* UF-WEB-001-15: Public User Account Password Policy
* UF-WEB-002-1: Assign TCPs
* UF-WEB-002-2: Request TCP acceptance
* UF-WEB-002-3: Notification for TCP assignment
* UF-WEB-002-4: Unassign TCPs
* UF-WEB-002-5: Temporary replacement of Head of Stream
* UF-WEB-002-6: Temporary replacement of TCP
* UF-WEB-002-7: Resignation of Head of Stream by BD officer
* UF-WEB-002-8: Notification of Head of Stream resignation
* UF-WEB-003-1: Listing out responsible Inspection Form
* UF-WEB-003-2: Listing out responsible Site-Monitoring Schemes
* UF-WEB-004-1: Form record submission and amendment
* UF-WEB-004-2: Search responsible Site Project
* UF-WEB-004-3: Create Site Project from the submitted Supervision plan
* UF-WEB-004-4: Edit and update Site Project Detail
* UF-WEB-004-5: List out Site Project
* UF-WEB-004-6: View Site Project Detail
* UF-WEB-004-7: Supervision Plan Detail View
* UF-WEB-004-8: Supervision Plan Detail Management
* UF-WEB-004-9: Import SMIS Excel into CDPSS

## 6. Equipment Configuration

### 6.1 Computer Hardware

#### 6.1.1 Hardware Components

**Hardware Components of Production Servers**

| Item | Hardware Component | Configuration | Qty |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Hardware Components of Disaster Recovery Servers**

| Item | Hardware Component | Configuration | Qty |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

#### 6.1.2 Guest Servers Components

**Production guest servers**

| Role | Host Name | vCPU | RAM (GB) | Disk (GB) | IP Addresses | Data Center | Host Server / Zone |
| --- | --- | --- | --- | --- | --- | --- | --- |
| vCenter | prd-scs-vcenter-01 | 16 | 39 | 1.33TB | 192.168.10.24 / 10.5.161.210 | WKGO | prd-scs-admin-server-01 |
| Veeam Backup Server | prd-scs-backup-01 | 8 | 24 | 300 + 1TB | 192.168.10.25 / 10.5.161.211 | WKGO | prd-scs-admin-server-02 |
| Kiwi Log Server | prd-scs-log-01 | 4 | 16 | 300 + 500 | 192.168.10.11 / 10.5.161.223 | WKGO | prd-scs-admin-server-01 |
| NOD32 Anti-Virus Server | prd-scs-esetnod32 | 4 | 16 | 300 | 192.168.10.34 / 10.5.161.215 | WKGO | prd-scs-admin-server-02 |
| API Server | prd-scs-admin-api-01 | 2 | 4 | 100 | 192.168.12.11 | WKGO | prd-scs-admin-server-01 |
| Frontend Server | prd-scs-admin-frontend-01 | 2 | 4 | 100 | 192.168.12.12 | WKGO | prd-scs-admin-server-01 |
| Backend Server | prd-scs-admin-backend-01 | 2 | 4 | 100 | 192.168.12.13 | WKGO | prd-scs-admin-server-01 |
| Database Server | prd-scs-db-01 | 8 | 16 | 100 + 500 | 192.168.12.14 | WKGO | prd-scs-admin-server-01 |
| File Server | prd-scs-filer | 2 | 4 | 100 + 1TB | 192.168.12.20 | WKGO | prd-scs-admin-server-01 |
| Reverse Proxy Server | prd-scs-proxy | 2 | 4 | 100 | 192.168.12.15 / 10.5.161.226 | WKGO | prd-scs-admin-server-01 |
| API Server | prd-scs-admin-api-02 | 2 | 4 | 100 | 192.168.12.16 | WKGO | prd-scs-admin-server-02 |
| Frontend Server | prd-scs-admin-frontend-02 | 2 | 4 | 100 | 192.168.12.17 | WKGO | prd-scs-admin-server-02 |
| Backend Server | prd-scs-admin-backend-02 | 2 | 4 | 100 | 192.168.12.18 | WKGO | prd-scs-admin-server-02 |
| Database Server | prd-scs-db-02 | 8 | 16 | 100 + 500 | 192.168.12.19 | WKGO | prd-scs-admin-server-02 |
| Reverse Proxy Server | scspwi | 2 | 8 | 100 | 192.168.0.6 / 45.119.92.84 | GCIS P1 | iDMZ |
| Reverse Proxy Server | scspwg | 2 | 8 | 100 | 192.168.4.6 / 10.160.11.211 | GCIS P1 | gDMZ |
| Apps Server | scspad | 4 | 16 | 100 + 500 | 192.168.8.6 | GCIS P1 | Trust Zone |
| Database Server | scspdb | 4 | 16 | 100 + 200 | 192.168.8.7 | GCIS P1 | Trust Zone |
| Veeam Backup Server | scspbk2 | 4 | 16 | 100 + 1TB | 192.168.8.9 | GCIS P1 | Trust Zone |
| Kiwi Log Server | scsplog | 2 | 8 | 100 + 100 | 192.168.8.10 | GCIS P1 | Trust Zone |

**UAT guest servers**

| Role | Host Name | vCPU | RAM (GB) | Disk (GB) | IP Addresses | Data Center | Host Server / Zone |
| --- | --- | --- | --- | --- | --- | --- | --- |
| API Server | uat-scs-admin-api-01 | 2 | 4 | 100 | 192.168.13.10 | WKGO | prd-scs-admin-server-01 |
| Frontend Server | uat-scs-admin-frontend-01 | 2 | 4 | 100 | 192.168.13.11 | WKGO | prd-scs-admin-server-01 |
| Backend Server | uat-scs-admin-backend-01 | 2 | 4 | 100 | 192.168.13.12 | WKGO | prd-scs-admin-server-01 |
| Database Server | uat-scs-db-01 | 2 | 4 | 100 | 192.168.13.13 | WKGO | prd-scs-admin-server-01 |
| File Server | uat-scs-filer | 2 | 4 | 100 + 200 | 192.168.13.15 | WKGO | prd-scs-admin-server-01 |
| Reverse Proxy Server | uat-scs-proxy | 2 | 4 | 100 | 192.168.13.14 / 10.5.161.224 | WKGO | prd-scs-admin-server-01 |
| Reverse Proxy Server | scsuwi | 2 | 8 | 100 | 192.168.0.7 / 45.119.94.99 | GCIS T1 | iDMZ |
| Reverse Proxy Server | scsuwg | 2 | 8 | 100 | 192.168.4.7 / 10.148.11.220 | GCIS T1 | gDMZ |
| Apps Server | scsuad | 4 | 16 | 100 + 200 | 192.168.8.9 | GCIS T1 | Trust Zone |
| Database Server | scsudb | 4 | 16 | 100 + 100 | 192.168.8.10 | GCIS T1 | Trust Zone |

**DEV guest servers**

| Role | Host Name | vCPU | RAM (GB) | Disk (GB) | IP Addresses | Data Center | Host Server / Zone |
| --- | --- | --- | --- | --- | --- | --- | --- |
| API Server | dev-scs-admin-api-01 | 2 | 4 | 100 | 192.168.14.10 | WKGO | prd-scs-admin-server-02 |
| Frontend Server | dev-scs-admin-frontend-01 | 2 | 4 | 100 | 192.168.14.11 | WKGO | prd-scs-admin-server-02 |
| Backend Server | dev-scs-admin-backend-01 | 2 | 4 | 100 | 192.168.14.12 | WKGO | prd-scs-admin-server-02 |
| Database Server | dev-scs-db-01 | 2 | 4 | 100 | 192.168.14.13 | WKGO | prd-scs-admin-server-02 |
| File Server | dev-scs-filer | 2 | 4 | 100 + 200 | 192.168.14.15 | WKGO | prd-scs-admin-server-02 |
| Reverse Proxy Server | dev-scs-proxy | 2 | 4 | 100 | 192.168.14.14 / 10.5.161.225 | WKGO | prd-scs-admin-server-02 |
| Reverse Proxy Server | scsdwi | 2 | 8 | 100 | 192.168.0.6 / 45.119.94.100 | GCIS T1 | iDMZ |
| Reverse Proxy Server | scsdwg | 2 | 8 | 100 | 192.168.4.6 / 10.148.11.220 | GCIS T1 | gDMZ |
| Apps Server | scsdad | 4 | 16 | 100 + 200 | 192.168.8.7 | GCIS T1 | Trust Zone |
| Database Server | scsddb | 4 | 16 | 100 + 100 | 192.168.8.8 | GCIS T1 | Trust Zone |

**Disaster Recovery guest servers**

| Role | Host Name | vCPU | RAM (GB) | Disk (GB) | IP Addresses | Data Center | Host Server / Zone |
| --- | --- | --- | --- | --- | --- | --- | --- |
| vCenter | dr-scs-vcenter-01 | 16 | 39 | 1.33TB | 192.168.20.18 / 10.5.174.225 | AIA | dr-scs-admin-server-01 |
| Veeam Backup Server | dr-scs-backup-01 | 8 | 24 | 300 + 1TB | 192.168.20.19 / 10.5.161.224 | AIA | dr-scs-admin-server-01 |
| Kiwi Log Server | dr-scs-log-01 | 4 | 8 | 300 + 500 | 192.168.20.10 | AIA | dr-scs-admin-server-01 |
| API Server | dr-scs-admin-api-01 | 2 | 8 | 90 | 192.168.22.11 | AIA | dr-scs-admin-server-01 |
| Frontend Server | dr-scs-admin-frontend-01 | 2 | 8 | 90 | 192.168.22.12 | AIA | dr-scs-admin-server-01 |
| Backend Server | dr-scs-admin-backend-01 | 2 | 8 | 90 | 192.168.22.13 | AIA | dr-scs-admin-server-01 |
| Database Server | dr-scs-db-01 | 2 | 8 | 90 + 500 | 192.168.22.14 | AIA | dr-scs-admin-server-01 |
| File Server | dr-scs-filer | 2 | 8 | 90 + 1TB | 192.168.22.16 | AIA | dr-scs-admin-server-01 |
| Reverse Proxy Server | dr-scs-proxy | 2 | 4 | 90 | 192.168.22.15 / 10.5.174.228 | AIA | dr-scs-admin-server-01 |

### 6.1.3 Gateway and SMTPX Configuration

**SMTPX**

| Item | Description |
| --- | --- |
| SMTPX service hostname | smtpx.cis.hksarg (resolvable by CCGO DNS) |
| SMTPX service IP address | 10.106.5.103, 10.106.5.104, 10.106.105.103, 10.106.105.104 (IP addresses are provided for ACL settings. To enjoy the automatic failover feature, mail servers should access SMTPX service through hostname.) |
| SMTP port number | 587 |
| Sender IP address | (B/Ds' IP address within GNET) |
| Login and password | Not required |
| Authentication | By e-Certificate issued from Hong Kong Post or the Government ISCCA |
| Sender address in e-mail | Valid e-mail address registered in IMX service |
| Connection encryption | STARTTLS (Mandatory) |
| Compatible Protocols | SPF and DKIM |

SMTPX configured in the IIS 6.0 of the following servers

scspwg, scsuwg, scsdwg

**WKGO Production Network Gateway**

| Gateway | Subnet | IP Range | vlan / Zone |
| --- | --- | --- | --- |
| 192.168.10.1 | 255.255.255.0 | 192.168.10.1-254 | Management |
| 192.168.11.1 | 255.255.255.0 | 192.168.11.1-254 | Replication / Backup |
| 192.168.12.1 | 255.255.255.0 | 192.168.12.1-254 | Production |
| 192.168.13.1 | 255.255.255.0 | 192.168.13.1-254 | UAT |
| 192.168.14.1 | 255.255.255.0 | 192.168.14.1-254 | DEV |
| 10.5.161.1 | 255.255.255.0 | 10.5.161.205-235 | BD Network |

**AIA DR Network Gateway**

| Gateway | Subnet | IP Range | vlan / Zone |
| --- | --- | --- | --- |
| 192.168.20.1 | 255.255.255.0 | 192.168.20.1-254 | Management |
| 192.168.21.1 | 255.255.255.0 | 192.168.21.1-254 | Replication / Backup |
| 192.168.22.1 | 255.255.255.0 | 192.168.22.1-254 | Production |
| 10.5.174.1 | 255.255.255.0 | 10.5.174.215-234 | BD Network |

#### 6.1.4 Database Configuration

* WKGO Production:
  + Windows Cluster: prd-scs-db-cl-01 192.168.12.21
  + Database Availability Group: prd-scs-db-agl 192.168.12.22
  + Replicas:
    - prd-scs-db-01 192.168.12.14 (Primary)
    - prd-scs-db-02 192.168.12.19 (Secondary)
* WKGO UAT:
  + Database: uat-scs-db-01 192.168.13.13
* WKGO DEV:
  + Database: dev-scs-db-01 192.168.14.13
* AIA DR:
  + Database: dr-scs-db-01 192.168.22.14
* GCIS P1:
  + Database: scspdb 192.168.8.7
* GCIS UAT:
  + Database: scsudb 192.168.8.10
* GCIS DEV:
  + Database: scsddb 192.168.8.8
* GCIS P2 DR:
  + Database: scspdb 192.168.8.7

#### 6.1.5 Detailed Server and Network Configurations

* Rack diagram
* External firewall
* Internal firewall
* Windows NLB
* Switches - Prod DMZ Port
* Switches - Prod INT SW Port
* Switches ? DR DMZ SW Port
* Switches ? DR INT SW Port

## 7. Software Inventories

### 7.1 Inventory of Application Programs

For details of Application Programs for LSCP, please refer to Program Manual (T352).

### 7.2 Inventory of System Software and Software Package

**System Software of Production**

| Machine | Hostname | Software |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Production**

| Item | Software Component | Qty |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**System Software of DR**

| Machine | Hostname | Software |
| --- | --- | --- |
| Kiwi Log Servers |  |  |
| Antivirus Server |  |  |
| DR Web Server (Static Content) 1 |  |  |
| DR Web Application Server 1 |  |  |
| DR BD Web Server 1 |  |  |
| DR Database Server (SQL Server) 1 |  |  |
| Backup Server |  |  |
| vCenter Server |  |  |
| VM Host |  |  |
| VM Host |  |  |

**DR**

| Item | Software Component |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**System Software of UAT**

| Machine | Hostname | Software |
| --- | --- | --- |
| UAT Web Server (Static Content) |  |  |
| UAT Web Application Server |  |  |
| UAT BD Web Server |  |  |
| UAT Database Server (SQL Server) |  |  |

**UAT**

| Item | Software Component |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## 8. Security and Backup

### 8.1 System Control

* The LSCP is protected by password control. BD users can log in via DP or the internet, requiring a one-time password (OTP) via Authenticator when logging in from the internet.
* External users log in via the internet or the iAM Smart app, requiring an OTP via email or using iAM Smart.
* User access rights are controlled based on their role.

### 8.2 Backup

* Production, UAT, and DEV environments on WKGO and DR on AIA are backed up by dedicated backup servers.
* Daily VM image backups are stored in backup storage, with weekly backups to tape and daily copies to AIA.
* Production environments on GCIS P1 are backed up by GCIS-provided backup services and replicated to DR GCIS P2.
* Database servers perform local database backups, which are then backed up by the Veeam backup server.

### 8.3 Security

#### 8.3.1 Data Transmission Security

Data transmission is encrypted using HTTPS over TLS. Public SSL certificates from HK Post are used on public-facing servers, while self-generated certificates secure the availability group.

#### 8.3.2 Data Storage and Auditing Security

Data is stored in SAN storage with RAID mirroring. Access and audit controls are strictly enforced, and data is encrypted. Audit trails record all data modifications.

#### 8.3.3 System Security

Regular security patches are applied to operating systems and software. Antivirus clients are installed on all servers and managed by a centralized Antivirus Management server.

#### 8.3.4 Physical Security

Servers and equipment are located in secure server rooms compliant with IT security guidelines.

#### 8.3.5 Password and Group Control

* Password complexity and policy follow the latest IT Security
* Guidelines.
* User access is restricted based on assigned roles.

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

* New users must register. Certain roles require providing
* registration numbers.
* External users use One-Time-Password tokens for secure login.
* Data submitted by TCP staff is vetted by Head of Stream staff.
* Application Maintenance Team access to production servers requires
* approval and is monitored by ITU.

### 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. Virtual machines undergo daily overnight backups, retained for 30 days.
* **BDSCS External (On-Prem):** NGINX Reverse Proxy/Load Balancer
* distributes traffic across two servers. Daily database backups are transferred to the production backup server. VM replication to DR environment is ensured using the VEEAM architecture.

### 8.6 Database Backup Strategy

#### 8.6.1 SQL Database Backup

Database full export backups are performed daily on database servers.

#### 8.6.2 Recovery

The table below shows the impact, system recovery and the expected duration before the BDSCS is resumed to normal operation when various system failures occur.

| # | Failure Scenario | Impact | System Recovery | Total down time |
| --- | --- | --- | --- | --- |
| 1 | System (hardware) failure of the primary database server | Production BDSCS services not available; All BDSCS users cannot use BDSCS | Pilot BDSCS needs to be setup using standby DB | ~1 hour |
| 2 | Electricity shortage on primary site | Production BDSCS services not available; All BDSCS users cannot use BDSCS | BDSCS needs to be setup using DR site | ~half day |
| 3 | System failure of either one of the App servers on primary site | According to the number of concurrent user, the performance may be degraded. | No effect on system availability | N/A |
| 4 | System failure of ALL App servers on primary site | Production BDSCS Web services not available; ALL BDSCS Web users cannot use BDSCS | BDSCS needs to be restored using App servers VM image backup | ~half day |
| 5 | Database connection failure since SQL database instance down | BDSCS services not available; ALL BDSCS users cannot use BDSCS | Restart SQL database instance | ~1 hour |
| 6 | Primary database crushed | No impact as it will failover to the secondary database |  |  |