**HANDOVER PLAN**

**FOR**

**COMBINED SYSTEM DEVELOPMENT SERVICES**

**FOR**

**LICENSING SELF-CERTIFICATION PORTAL**

**FOR**

**BUILDINGS DEPARTMENT**

**Version: 0.1**

**Jan 2025**

? The Government of the Hong Kong Special Administrative Region

The contents of this document remain the property of, and may not be reproduced in whole or in part without the express permission of the Government of the HKSAR.

| **Distribution** |  |
| --- | --- |
| Copy No. | Holder |
| 1 | Buildings Department (BD) |
| 2 | Master Concept (Hong Kong) Limited (MC) |

## Amendment History

| Change Number | Revision Description | Pages Affected | Revision Number | Date | Approved Reference |
| --- | --- | --- | --- | --- | --- |
| 1 | 1st draft | All | 0.1 | 16/01/2024 |  |
|  |  |  |  |  |  |

## TABLE OF CONTENTS

[1. Environment Description](#environment-description) [2. Purpose](#purpose) [2.1 Schedule](#schedule) [2.2 Verification](#verification) [3. Documentation](#documentation) [4. Program Source Code](#program-source-code) [5. Administration Accounts Checklist](#administration-accounts-checklist) [6. Backup](#backup) [6.1 VM Backup](#vm-backup) [6.2 Database Backup](#database-backup) [7. Outstanding Items/Issues](#outstanding-itemsissues) [8. Licensed Software](#licensed-software) [9. System Summary](#system-summary) [9.1 Objective](#objective) [9.2 System Architecture](#system-architecture) [9.3 System Functions](#system-functions) [10. Equipment Configuration](#equipment-configuration) [10.1 Computer Hardware](#computer-hardware) [10.1.1 Hardware Components](#hardware-components) [10.1.2 Guest Servers Components](#guest-servers-components) [10.1.3 Gateway and SMTPX Configuration](#gateway-and-smtpx-configuration) [10.1.4 Database Configuration](#database-configuration-sm) [10.1.5 Detailed Server and Network Configurations](#X5c8787595098517947b6f23ac38f4fe7cded31c) [10.2 Software Inventories](#software-inventories) [10.2.1 Inventory of Application Programs](#inventory-of-application-programs) [10.2.2 Inventory of System Software and Software Package](#X81b4f3a47ed49f46e508cb8e84d3c9c1e3bcbc0) [11. Security and Backup Details](#security-and-backup-details) [11.1 System Control](#system-control) [11.2 Backup Details](#backup-details) [11.3 Security Details](#security-details) [11.3.1 Data Transmission Security](#data-transmission-security) [11.3.2 Data Storage and Auditing Security](#data-storage-and-auditing-security) [11.3.3 System Security](#system-security) [11.3.4 Physical Security](#physical-security) [11.3.5 Password and Group Control](#password-and-group-control) [11.3.6 Control Procedure of Application User Account and Production Support Account](#X51231f61d13e098c78085aaed4438a02843607e) [11.4 Change Control](#change-control) [11.5 Disaster Recovery](#disaster-recovery) [11.6 Database Backup Strategy](#database-backup-strategy) [11.6.1 SQL Database Backup](#sql-database-backup-strategy) [11.6.2 Recovery](#recovery-strategy) [11.6.3 Backup Schedule](#backup-schedule-strategy) [12. Database Administration](#database-administration-section) [12.1 Clean Database Transaction Logs](#clean-database-transaction-logs) [12.2 Database Backup Procedure](#database-backup-procedure) [13. System Constraints and Limitations](#system-constraints-and-limitations) [14. Log Management](#log-management)

# 1. Environment Description

**Production and UAT environment:**

[an image here]

**List of machines and virtual machines:**

**DR environment:**

[image here]

**List of machines and virtual machines:**

# 2. Purpose

This document is a checklist of handover materials within project scope and provides relevant information to the support maintenance staffs who will be maintaining this system in the future. All these deliverables should be received from system implementation team of the Licensing Self-Certification Portal (LSCP) to the Buildings Department (BD) of the Government of the Hong Kong Special Administrative Region (HKSARG or the Government).

The hand-over items of this project can be summarized into the following items:

1. Documentation
2. Program Source code (Backend Application, Frontend Web App, Fronted Mobile App)
3. Administration Accounts
4. System backup
5. Hardware
6. Software Packages and Licenses

## 2.1 Schedule

| Action | Date | Action Parties |
| --- | --- | --- |
| Handover |  | MC/BD |
| Verification |  | BD |

## 2.2 Verification

1. **The application URL verification**

* The access link (URL) of each application should be verified by performing an access checking.

1. **Login accounts verification**

* The login accounts of the applications and servers should be verified by processing login action.

# 3. Documentation

| Document | File Name | Version |
| --- | --- | --- |
| SA&D Report |  |  |
| Project Initiation Document (PID) |  |  |
| Physical Data Design |  |  |
| Process Data Interface |  |  |
| Data Catalogue |  |  |
| Program Specifications |  |  |
| Performance Optimization Report |  |  |
| System Test Plan, Spec and Results |  |  |
| Unit Test Cases and Results |  |  |
| Load Test Plan and Result |  |  |
| Training Plan |  |  |
| User Manual |  |  |
| System Installation Plan Report |  |  |
| DR Plan |  |  |
| DR Drill Test result Report |  |  |
| WCAG |  |  |
| UAT Plan and Results |  |  |
| Application Operation manual |  |  |
| Computer Operation Procedures Manual |  |  |
| Data Manual |  |  |
| System Maintenance Plan |  |  |
| User Procedures Manual |  |  |
| Security Incident Handling Procedure |  |  |
| Handover Plan |  |  |
| System Manual |  |  |
| Program Manual |  |  |
| Project Evaluation Report |  |  |

# 4. Program Source Code

| Component | Machine | Directory |
| --- | --- | --- |
| Frontend Application |  |  |
| Backend Application |  |  |
|  |  |  |

# 5. Administration Accounts Checklist

In this section, it will list the user account for management in the different areas.

**Administration Accounts on LSCP**

| Environment | User Type | User account | Password |
| --- | --- | --- | --- |
| UAT | BD Admin |  |  |
| PRD / DR | BD Admin |  |  |
|  |  |  |  |

# 6. Backup

[RY Note: Following content needs to check]

## 6.1 VM Backup

Backup service is carried out by backup server.

Daily VM image backup is carried out and store in the backup servers. A further copy of production VM images is copied to DR?s backuper server.

## 6.2 Database Backup

Database full export backup: this type of backup contains full database exported database objects including schemas, table structures, packages, stored procedures and data.

Daily full export backup is done on DB servers, data stored on the DB servers and further backed up by VM Backup.

# 7. Outstanding Items/Issues

Nil.

# 8. Licensed Software

[RY Note: Items are for reference only. They are incorrect]

| Item | Amount | Expire At |
| --- | --- | --- |
| Windows 2022 Standard (16-Core) - Perpetual |  |  |
| SQL 2019 Standard (2-Core) - Perpetual |  |  |
| Veeam Availability Suite Universal License (10-Instance) with 3 year prod support |  |  |
| Symantec SEP License (3 years) |  |  |
| Kiwi Log Servers (with 3 year support & subscription) |  |  |
| vSphere Standard (basic Support with 3years SNS) |  |  |
| vCenter Standard (basic Support with 3years SNS) |  |  |

# 9. System Summary

## 9.1 Objective

The users of the LSCP can be classified into two categories:

* BD Officers
* Public users involved in site inspection and site monitoring

The primary objective of LSCP is to provide an electronic platform for site inspection and site monitoring personnel to provide, manage, and review the inspection and monitoring records.

## 9.2 System Architecture

This is an overview of the system structure of LSCP in the Production Environment.

The following diagram illustrates the architecture of the LSCP for Production site and UAT site in another perspective.

The system is holding on two datacenters: On-premise (WKGO) and Government Cloud Infrastructure Services (GCIS).

The On-premise system is behind an internal firewall that uses NAT to separate into 3 subnets. There are Production, UAT and DEV for internal users only.

A reverse proxy server with load balancing function is used for increased security and share the incoming requests to the frontend web servers.

The system on GCIS is divided into 3 subnets: Internet DMZ (iDMZ), Trusted Zone and Gnet DMZ (gDMZ).

Both iDMZ and gDMZ contain a reverse proxy server and a Web Application Firewall (WAF) also deployed in front of the iDMZ for increased security access.

External users (i.e. public users) access the system from the internet through the internet using LSCP Web Application, which interacts with the Application Server through the reverse proxy server. The Application Server hosts the static web interface files.

To perform system logic, the External Application Servers will pass requests to the Web Servers in the Trusted Zone. The web application, written in reactjs, will interact with the external web server that is written in nodeJS that in turns perform CRUD on the Database Servers, which host Microsoft SQL Servers, and the in-built file storage to perform logic computing, and return result to the External Web Servers then to the internet.

In addition to external users, internal users who would access the internal BDSCS application from BD intranet, would connect to the BD Web Servers in the Trusted Zone, through the Departmental Portal (OSDP). The BD Web Servers perform the same function as the External Web Servers and perform user authentication functions when interfaced with the Departmental Portal.

Finally, there are some more servers in the Trusted Zone to support internal BDSCS application, which includes:

* Log Server to store the system and application log from other servers
* File Server to store the temporary and permanent files
* Database Server that hosts Microsoft SQL server to store all the system and user information
* vCenter Server to manage the VM Hypervisors on each of the physical servers
* Backup Server to keep snapshots of the database

Below are further details of each of the system components in the BDSCS:

**External Application Server**

The external application servers serve the static web contents in form of HTML, CSS, and JavaScript to the internet, through Microsoft's Internet Information Services (IIS), and also proxy the backend APIs (GraphQL format) to the web application servers as being in the DMZ.

The website hosted on the external web servers is written in JavaScript under the React framework. After compiling the JavaScript project, the result files are stored in the external web servers and served by IIS, with rewrite rules to proxy the backend APIs.

**External Web Server**

The external web server, in this context, refers to a server that hosts and runs the backend API responsible for processing business logic and performing database operations. In the case of IIS (Internet Information Services) and expressJS, IIS serves as the web server software, while ExpressJS represents the framework used for developing the backend APIs.

The backend API, developed using ExpressJS, encompasses the code that handles various tasks, including interacting with databases, executing business logic, and processing requests from clients. It acts as the intermediary between the frontend (such as a mobile or web application) and the underlying data storage.

When a client application makes a request to the backend API, IIS receives the request and passes it to the appropriate ExpressJS code for processing. The backend API then performs the necessary operations, which may involve querying the database, executing business rules, or performing calculations. Once the processing is complete, the backend API generates a response that is sent back to the client application (External Application Server in this case) through IIS.

**BD Web Servers**

The BDSCS backend portal was developed for internal BD users and BD ITU. It is using the same technology stack as Extra Application Server but just deployed to different zones to ensure security and connectivity for internal BD users only

**Database Management Servers**

Both the internal and external BDSCS applications are built on the Microsoft SQL Server database engine.

**Web Browser Support**

**iAM Smart**

The iAM Smart system implemented by the Government of Hong Kong focuses primarily on providing a secure and convenient login mechanism and retrieving basic user information. Pilot CDPSS has integrated with iAM Smart authentication module. Users can utilize iAM Smart to log in to Pilot CDPSS services and retrieve basic information associated with their digital identity.

**Departmental Portal**

The Departmental Portal is a web service of BD to pass BD user?s identity to other wb services including the LSCP. When BD users access LSCP website through the Departmental Portal, the user ID will be provided to the LSCP to complete the login process without further input from the user. This login method only available inside BD?s network.

**SMTPX**

The notification module in BDSCS would send login one-time password (OTP) and email notification by initiating an SMTPX service provided by CIS.

**MWMS**

MWMS would provide data of AP/RSE/RGE/AS acknowledged by BD. Snapshots of the MWMS data will be interfaced to BDSCS through SFTP and then internal and external BDSCS applications would intake this data by processing the batch file auto-generated and delivered from MWMS daily.

**BCIS**

BCIS would provide address data and BD case data acknowledged by BD. The latest copy of the BCIS database would be synced to BDSCS through SQL queries at midnight. The data would then be used in both external and internal portals for address selection, folio management, and case logic. Meanwhile, the new BD cases would be synced to BCIS in real time through a SQL stored procedure.

This is an overview of the system structure of Pilot CDPSS in Disaster Recovery Environment, similar with the production environment

## 9.3 System Functions

| Function ID | Function Name |
| --- | --- |
| 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 |

# 10. Equipment Configuration

## 10.1 Computer Hardware

### 10.1.1 Hardware Components

**The Configuration of Physical Server in Production**

| Model | Host Name | IP | Serial No. | Disk Configuration |
| --- | --- | --- | --- | --- |
| Dell PowerEdge R750 Server | prd-scs-admin-server-01 | 192.168.10.22, 10.5.161.206 | F646RX3 | RAID-5 |
| Dell PowerEdge R750 Server | prd-scs-admin-server-02 | 192.168.10.23, 10.5.161.207 | D646RX3 | RAID-5 |
| Dell PowerEdge R750 Server | prd-scs-nas | 192.168.10.35, 10.5.161.218 | ??? | ??? |

**The Configuration of SAN storage in Production**

| Type | Model | Serial No. | No. of hard disks | IP Address |
| --- | --- | --- | --- | --- |
| SAN Switch | Dell DS6610B | FRC1924T0CC | N/A | 192.168.10.16 |
| SAN Switch | Dell DS6610B | FRC1924T0CD | N/A | 192.168.10.17 |
| SAN Storage | Dell PowerStore 500T | HV1NBX3 | 11 | 192.168.10.26, 192.168.10.27, 192.168.10.28, 192.168.10.29 |

**The Configuration of Backup storage in Production**

| Type | Model | Serial No. | Volume Size | IP Address |
| --- | --- | --- | --- | --- |
| Backup Appliance | Dell DataDomain 3300 | 17XMBX3 | 15TB | 192.168.10.20 |

**The Configuration of Tape Library in Production**

| Type | Model | Serial No. | No. of slots | IP Address |
| --- | --- | --- | --- | --- |
| Tape Library | Dell ML3 | 3555L3A7801YY0 | 35 | 192.168.10.20 |

**The Configuration of Firewalls in Production**

| Host Name | Internal IP | External IP | Model | Serial No. |
| --- | --- | --- | --- | --- |
| PA-850-SCSPri | 192.168.10.12 | 10.5.161.205 | Palo Alto PA-850 | 11901063047 |
| PA-850-SCSSec | 192.168.10.13 | 10.5.161.220 | Palo Alto PA-850 | 11901063049 |

**The Configuration of switches in Production**

| Host Name | Internal IP | Model | Serial No. |
| --- | --- | --- | --- |
|  | 192.168.10.14 | Catalyst |  |
|  | 192.168.10.15 | Catalyst |  |

**The Configuration of KVM in Production**

| Model | Serial No. |
| --- | --- |
| Cyber View |  |

**The Configuration of UPS in Production**

| Model | Serial No. | IP Address |
| --- | --- | --- |
| Vertiv? Liebert? GXT5 3000 | 2102311887222A010008 | 192.168.11.20 |
| Vertiv? Liebert? GXT5 3000 | 2102311887222A010004 | 192.168.11.21 |

**Hardware Components of Production Servers**

| Item | Hardware Component | Configuration | Qty |
| --- | --- | --- | --- |
| 1 | ESXi Hypervisor Server (prd-scs-admin-server-01) | Dell PowerEdge R750 | 1 |
|  |  | Intel(R) Xeon(R) Gold 6326 CPU @ 2.90GHz | 1 |
|  |  | 32GB DDR4 Synchronous Registered (Buffered) | 8 |
|  |  | 1.2TB SAS HDD | 3 |
|  |  | ESXi 8.0.3 | 1 |
| 2 | ESXi Hypervisor Server (prd-scs-admin-server-02) | Dell PowerEdge R750 | 1 |
|  |  | Intel(R) Xeon(R) Gold 6326 CPU @ 2.90GHz | 1 |
|  |  | 32GB DDR4 Synchronous Registered (Buffered) | 8 |
|  |  | 1.2TB SAS HDD | 3 |
|  |  | ESXi 8.0.3 | 1 |
| 3 | NAS (prd-scs-nas) | Dell PowerEdge R750 | 1 |
|  |  | CPU??? | ??? |
|  |  | RAM??? | ??? |
|  |  | HDD??? | ??? |
|  |  | Windows Server 2022 | ??? |
| 4 | SAN Switch (prd-scs-sw-01) | Dell DS6610B | 1 |
|  |  | Ports | 16 |
| 5 | SAN Switch (prd-scs-sw-02) | Dell DS6610B | 1 |
|  |  | Ports | 16 |
| 6 | SAN Storage (PS500T-Cluster1) | Dell PS500T | 1 |
|  |  | 3.8TB NVME SSD | 11 |
| 7 | Backup Appliance (prd-scs-backupstorage-01) | Dell DataDomain DD3300 | 1 |
| 8 | Tape Library | DELL ML3 | 1 |
| 9 | Firewall (PA-850-SCSPri) | Palo Alto PA 850 | 1 |
| 10 | Firewall (PA-850-SCSSec) | Palo Alto PA 850 | 1 |
| 11 | Switch (???) | Cisco ??? | 1 |
| 12 | Switch (???) | Cisco ??? | 1 |
| 13 | KVM | CyberView | 1 |
| 13 | UPS (???) | Vertiv? Liebert? GXT5 3000 | 1 |
| 14 | UPS (???) | Vertiv? Liebert? GXT5 3000 | 1 |

**Partition Configuration of Production Servers**

| Host Name | Drive | Capacity | Description |
| --- | --- | --- | --- |
| prd-scs-admin-server-01 | local | 2.4TB | VMware ESXi Operating system |
| prd-scs-admin-server-02 | local | 2.4TB | VMware ESXi Operating system |
| PS500T-Cluster1 | VM\_Volume01 | 20TB | Shared pool of storage space |
| PS500T-Cluster1 | QuorumDisk-VM-1 | 2.5GB | Shared pool of storage space |
| prd-scs-nas | C: | ??? | OS |
|  | D: | ??? | Data |

**The Configuration of Physical Server in DR Site**

| Model | Host Name | IP | Serial No. | Disk Configuration |
| --- | --- | --- | --- | --- |
| Dell PowerEdge R750Server | dr-scs-admin-server-01 | 192.168.20.17, 10.5.174.216 | G646RX3 | RAID-5 |
| Dell PowerEdge R750Server | dr-scs-nas | 192.168.20.35, 10.5.174.225 | ??? | ??? |

**The Configuration of SAN storage in DR Site**

| Type | Model | Serial No. | No. of hard disks | IP Address |
| --- | --- | --- | --- | --- |
| SAN Switch | Dell DS6610B | FRC1924T0CE | N/A | 192.168.20.14 |
| SAN Storage | Dell PowerStore 500T | 3W1NBX3 | 11 | 192.168.20.20, 192.168.20.21, 192.168.20.22, 192.168.20.23 |

**The Configuration of Backup storage in Production**

| Type | Model | Serial No. | Volume Size | IP Address |
| --- | --- | --- | --- | --- |
| Backup Appliance | Dell DataDomain 3300 | J6XMBX3 | 15TB | 192.168.20.25 |

**The Configuration of Firewalls in DR Site**

| Host Name | Internal IP | External IP | Model | Serial No. |
| --- | --- | --- | --- | --- |
| PA-850-SCSDR | 192.168.20.12 | 10.5.174.215 | Palo Alto PA-850 | 011901063069 |

**The Configuration of Switches in DR Site**

| Host Name | Internal IP | Model | Serial No. |
| --- | --- | --- | --- |
| ??? | 192.168.20.13 | Catalyst ??? | ??? |

**The Configuration of UPS in DR Site**

| Model | Serial No. | IP Address |
| --- | --- | --- |
| Vertiv? Liebert? GXT5 3000 | 2102311887222A01000A | 192.168.20.11 |

**Hardware Components of Disaster Recovery Servers**

| Item | Hardware Component | Configuration | Qty |
| --- | --- | --- | --- |
| 1 | ESXi Hypervisor Server (dr-scs-admin-server-01) | Dell PowerEdge R750 | 1 |
|  |  | Intel(R) Xeon(R) Gold 6326 CPU @ 2.90GHz | 1 |
|  |  | 32GB DDR4 Synchronous Registered (Buffered) | 8 |
|  |  | 1.2TB SAS HDD | 3 |
|  |  | ESXi 8.0.3 | 1 |
| 2 | NAS (dr-scs-nas) | Dell PowerEdge R750 | 1 |
|  |  | CPU??? | ??? |
|  |  | RAM??? | ??? |
|  |  | HDD??? | ??? |
|  |  | Windows Server 2022 | ??? |
| 3 | SAN Switch (dr-scs-sw-01) | Dell DS6610B | 1 |
|  |  | Ports | 16 |
| 4 | SAN Storage (PS500T-Cluster2) | Dell PS500T | 1 |
|  |  | 3.8TB NVME SSD | 11 |
| 5 | Backup Appliance (dr-scs-backupstorage-01) | Dell DataDomain DD3300 | 1 |
| 6 | Firewall (PA-850-SCSPri) | Palo Alto PA 850 | 1 |
| 7 | Switch (???) | Cisco ??? | 1 |
| 8 | KVM | CyberView | 1 |
| 9 | UPS (???) | Vertiv? Liebert? GXT5 3000 | 1 |

**Partition Configuration of DR Servers**

| Host Name | Drive | Capacity | Description |
| --- | --- | --- | --- |
| dr-scs-admin-server-01 | local | 2.4TB | VMware ESXi Operating system |
| PS500T-Cluster2 | VM Volume01 | 20TB | Shared pool of storage space |
| dr-scs-nas | C: | ??? | OS |
|  | D: | ??? | Data |

### 10.1.2 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 | 192.168.1 |  |  |