```markdown

**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) |

**TABLE OF CONTENTS**

[1. Environment Description](#environment-description)

* [1.1. Production and UAT Environment](#production-and-uat-environment)
* [1.2. DR Environment](#dr-environment) [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)
* [6.3 Database Backup Strategy](#database-backup-strategy)
  + [6.3.1 SQL Database Backup](#sql-database-backup)
  + [6.3.2 Recovery](#recovery)
  + [6.3.3 Backup Schedule](#backup-schedule) [7. Outstanding Items/Issues](#outstanding-itemsissues) [8. Licensed Software](#licensed-software) [9. Security](#security)
* [9.1 System Control](#system-control)
* [9.2 Data Transmission Security](#data-transmission-security)
* [9.3 Data Storage and Auditing Security](#data-storage-and-auditing-security)
* [9.4 System Security](#system-security)
* [9.5 Physical Security](#physical-security)
* [9.6 Password and Group Control](#password-and-group-control)
* [9.7 Control Procedure of Application User Account and Production Support Account](#X51231f61d13e098c78085aaed4438a02843607e)
* [9.8 Change Control](#change-control)
* [9.9 Disaster Recovery](#disaster-recovery) [10. Log Management](#log-management) [11. Equipment Configuration](#equipment-configuration)
* [11.1 Computer Hardware](#computer-hardware)
  + [11.1.1 Hardware Components](#hardware-components-1)
  + [11.1.2 Guest Servers Components](#guest-servers-components-1)
  + [11.1.3 Gateway and SMTPX Configuration](#gateway-and-smtpx-configuration-1)
  + [11.1.4 Database Configuration](#database-configuration-1)
  + [11.1.5 Detailed Server and Network Configurations](#X5c8787595098517947b6f23ac38f4fe7cded31c)
* [11.2 Software Inventories](#software-inventories)
  + [11.2.1 Inventory of Application Programs](#inventory-of-application-programs-1)
  + [11.2.2 Inventory of System Software and Software Package](#Xd45513c0c296a44a2ca5d95cc2ec4f3b4dde69d) [12. Definitions and Conventions](#definitions-and-conventions)
* [12.1 Definitions](#definitions)
* [12.2 Conventions](#conventions) [13. System Summary](#system-summary)
* [13.1 Objective](#objective-1)
* [13.2 System Architecture](#system-architecture-1)
* [13.3 System Functions](#system-functions-1) [14. Database Administration](#database-administration-1)
* [14.1 Clean Database Transaction Logs](#clean-database-transaction-logs)
* [14.2 Database Backup](#database-backup-1)
* [14.3 System Constraints and Limitations](#system-constraints-and-limitations)

# 1. Environment Description

## 1.1. Production and UAT Environment

Production and UAT environment:

[Production and UAT environment diagram here. Please refer to source documents for images.]

List of machines and virtual machines:

## 1.2. DR Environment

DR environment:

[DR environment diagram here. Please refer to source documents for images.]

List of machines and virtual machines:

# 2. Purpose

This document is a checklist of handover materials within project scope; and it also provides relevant information to the support maintenance staff 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 6 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.

## 6.3 Database Backup Strategy

### 6.3.1 SQL Database Backup

Besides DB server VM backup, database full export backup will be carried out as well. This type of backup contains full database export database objects including schemas, table structures, packages, stored procedures and data at 18:45 daily.

The daily full export backup is done on DB servers (uat-db-01, prd-db-01, prd-db-02, dr-db-01), data stored on the DB servers? directory: D:\backup\

### 6.3.2 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.

### 6.3.3 Backup Schedule

|  |  |
| --- | --- |
| Name | Schedule |
| PROD VM Backup Job 3 Daily | Daily 12:01 AM (Full) |
| PROD VM Backup to Tape Job 3 Weekly | Every Sunday 09:00 AM (Full) |
| PROD UAT VM Backup Job 1 Daily | Daily 08:00 PM (Full) |
| PROD UAT VM Backup to Tape Job 1 Weekly | Every Sunday 06:00 AM (Full) |
| PROD DEV VM Backup Job 2 Daily | Daily 10:00 PM (Full) |
| PROD DEV VM Backup to Tape Job 2 Weekly | Every Sunday 03:00 AM (Full) |
| PROD All jobs to DR Backup Copy Job 1 | After every PROD VM Backup Job 1, 2 and 3 Daily |
| DR VM Backup Job 4 Daily | Daily 08:00 PM (Full) |

# 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. Security

## 9.1 System Control

There will be no change in the existing authentication mechanisms. BD staff would still be authenticated by the OSDP before they can access the LSCP. If OSDP is unavailable in some situations such as maintenance, the LSCP would itself authenticate the users by the username and password + one-time password.

As for external users, they will still be required to be authenticated by OTP sent via email.

Password complexity and policy will be updated to follow the latest IT Security Guidelines [G3].

The LSCP grants functions access rights to users based on their post, and only ?Responsible Officers? are allowed to maintain their own records.

## 9.2 Data Transmission Security

Data of the LSCP is classified to the ?Restricted? level. Data transmission over the network will be encrypted by HTTPS over TLS. In order to enable TLS on the web servers of the LSCP, certificates will be applied, OGCIO?s Intranet Server Certificate Certification Authority (ISCCA) certificate will be apply for securing servers, applications, and communications within BD internal network (intranet)., Public SSL certificates, from HK post are used on public-facing servers and websites, intended to be trusted by the general public over Internet. Self-generated cert is used to secure the availability group which contains 2 production databases. And iAM Smart cert are configured in LSCP backend application in order to work with iAM Smart Mobile App.

## 9.3 Data Storage and Auditing Security

Data of the LSCP in production environment is stored in SAN storage. On the other hand, data storage in DR environment is stored in local server storage, Access and audit controls to this folder or drive are strictly controlled. Both environments facilitated with RAID (Redundant Array of Inexpensive Disks or Redundant Array of Independent Disks) mirroring data storage technology and all data are encrypted, OS secured by RAID 1 while data secured by ADAPT and Raid 6. In terms of fault tolerance, ADAPT (Autonomic Distributed Allocation Protection Technology) and Raid 6 withstands the failure of 2 hard disks. Moreover, all data facilitated with audit trail, records add/ change/ delete actions reposted in database for tracking who/ when/ what data being amended.

## 9.4 System Security

Regular service pack and patch updates are performed on operating system and software installed in servers and user workstations in order to fix the known security issues.

All servers in both the production and DR environment will be installed with Antivirus clients and managed by a virtualised Antivirus Management server installed at Trust zone. The server will download the latest virus signatures from the antivirus software provider (Symantec) and update all client servers during non-peak hours. Protection policy, such as scanning schedule, will be enforced by the BD?s antivirus management server too.

The external users will be responsible for the security protection on their computers. Their computers will have personal firewall enabled, the latest security patches applied, and anti-virus protection and malicious code detection installed.

## 9.5 Physical Security

Servers and equipment of the development/testing, production and DR environments are located in the server rooms, which the server rooms setup compliant with the section 8 of IT Security Guidelines [G3] and section 5.8 of Data Centre Site Preparation Guidelines [G36] where applicable.

## 9.6 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.

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

If user is new to the LSCP, user is required to register. For certain role, such as head of stream, user is required to provide their Registered Professionals or Contractors registration number. And all public user is required to provide HKID and check versus our database.

For external users, the LSCP implemented One-Time-Password token as secure login approach so that they can access the LSCP from their working locations for submission and retrieval of assignment details, and inspection results.

All information submitted by low level TCP staff will be vetted by Head of stream staff before saving as finalized records on the system.

To deliver on-going production support or change request, Application Maintenance Team may require to access the production servers for cause investigation, system/ application log collection or change request deployment. The Application Maintenance Team should seek the System Maintenance Committee?s approval by email. With the proof of authorization, ITU can help to login the servers, after that the Application Maintenance Team operates on the servers under the ITU?s monitoring. In case, the information/ operation can only be accessed/ executed under particular system account, the Application Maintenance Team should ask system account holder or designated person (Business Coordination Team member) to logon for his action.

## 9.8 Change Control

During the SI&I stage, program source of the LSCP is maintained by the Application Maintenance Team with aid of GIT repository with version control, any updating on the program source is recorded for tracking of program changes. GIT will be continue using in the change control solution for the SM&S stage. For detail procedure, please refer to COPM.

## 9.9 Disaster Recovery

**GCIS**

Automatic Failover:

If GCIS Prod 1 goes down, the GCIS Prod 2 disaster recovery (DR) environment will be automatically activated by the VM Site Recovery Manager. After a brief delay, users will be directed to the temporary domain (www2) to continue their usage seamlessly

Virtual Machine Backups:

The virtual machines of GCIS Prod 1 will undergo daily overnight backups, with each backup retained for 30 days.

Daily Database Backup:

A cron job is scheduled to export the GCIS Prod 1 database backup to the backup server every day at 22:00.

**BDSCS External (On-Prem):**

Load Balancing with NGINX:

A NGINX Reverse Proxy/Load Balancer (running on ESXi) distributes traffic across two servers. In case one server becomes unavailable, traffic will automatically be redirected to the other server.

Scheduled Database Backup:

A cron job runs daily at 18:30 to export the database.

Backup Transfer:

At 19:00, the VM service will send the exported database backup to the production backup server.

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

# 10. Log Management

1. 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 (e.g., software configuration files, password and key files, etc.) ? 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

1. Logs shall be retained for **180 days** and centralised and managed by Syslog server. Unauthorised access is restricted.
2. Logs will be reviewed regularly.
3. Logs shall not be used to profile the activity of a particular user unless it relates to a necessary audit activity supported by a Directorate rank officer.

# 11. Equipment Configuration

## 11.1 Computer Hardware

### 11.1.1 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.** |