BUSINESS CONTINUITY PLAN & BACKUP PLAN

ON

DATA MANAGEMENT SYSTEM

FOR

BUILDINGS ENERGY EFFICIENCY ORDINANCE

FOR

ENERGY EFFICIENCY OFFICE

OF

ELECTRICAL AND MECHANICAL SERVICES DEPARTMENT (EMSD)

機電工程署
EMSD

By

AUTOMATED SYSTEMS (HK) LTD.
自 動 系 統 （ 香 港 ） 有 限 公 司

Version: 0.1

July 2022

Distribution	
Copy No.	Holder
1	Electrical and Mechanical Services Department (EMSD)
2	Automated Systems (HK) Limited (ASL)

Prepared By: _____
Christine LAM
Automated Systems (HK) Ltd.
[Project Manager]

Date: _____

Endorsed By: _____
Kenneth Fung
Electrical and Mechanical Services Department
[EE/ITD/3]

Date: _____

Amendment History				
Change Number	Revision Description	Section Affected	Revision Number	Date
1	Draft Version	All	0.1	06/07/2022

TABLE OF CONTENTS

1 INTRODUCTION

This Business Continuity Plan (BCP) provides a documented framework including the management organization and procedures for monitoring, activation, deactivation, communication and actions to be followed during loss, interruption or disruption of mission-critical functions of Data Management System for Buildings Energy Efficiency Ordinance (DMS-BEEO).

2 SCOPE

The guidelines outlined in this document, though not intended to be restrictive and exhaustive process to cover every business continuity scenario for DMS of BEEO, they have covered the continuity planning for mission-critical functions.

3 DEFINITION AND CONVENTION

3.1 DEFINITIONS

In this document, unless the context otherwise requires, the following expressions have the following meanings:

Term	Definition
BEEO	Electricity Ordinance Regulation System
ASD	Architectural Services Department, it is requested to repair or rebuild the damaged computer site. They are coordinated by the Chief DR Commander.
DR Drill	The drill to practice the flow and activities defined in the Disaster Recovery Plan, so as to spot out the problem resided in the DR Plan, hence made the actual Disaster Recovery become smooth.
Contingency	The major disruption to the services of DMS BEEO that lead to unavailability of the mission-critical functions for an estimated duration acceptable system down time.
Acceptable system down time	The time period accepted and agreed between EMSD CMT and DMS BEEO end users for unavailable services from LEO III. The said time period is defined as 24 hours.
Target recovery time	The time period aimed by EMSD CMT to recover DMS BEEO services to end users. The said time period is defined as 72 hours.

4 IMPACT AND THREAT ANALYSIS

DMS BEEO can be affected by various threats, such as natural disasters, computer virus, hacking activities, hardware malfunctioning, networking failure, power shortage, and other sudden outage of supportive services.

Based on the possible threats to DMS of BEEO, the following major impacts to the mission-critical activities of DMS of BEEO are defined, and the detail scenario descriptions, solution and implementation planning are mentioned in Section 5 “Impact Scenario, Solution and Implementation”.

Scenario A : Disaster in Watson Centre, Kwai Chung (e.g. fire, floods, explosion)

Scenario B : Loss of power supply in EMSD server room

Scenario C : Damage and malfunctioning of DMS of BEEO servers

Scenario D : Security attacks (e.g. hackers, computer viruses, unauthorized access)

Scenario E : Network service failure

5 IMPACT SCENARIO, SOLUTION AND IMPLEMENTATION

In response to the threats identified in the section above, the scenario, solution and the actions to take are described as follow:

5.1 SCENARIO A : DISASTER IN WATSON CENTRE, KWAI CHUNG

Scenario	Fire, floods, explosion disrupting Watson Centre, Kwai Chung
Impact	Affects the safety of human lives and facilities, and the operation of DMS BEEO hosted in Watson Centre, Kwai Chung
Related Parties	[POST 1], [POST 2], [POST 4]
Monitoring, Activation / Deactivation	• Upon receiving any report of incidents, [POST 1] is required to closely monitor the incident and determine the impacts to the operations of DMS BEEO. • If [POST 4] finds that the agreed mission-critical activities cannot be performed, [POST 4] should report the situation to [POST 2] and review if BCP of DMS BEEO need to be activated. • [POST 2] will seek approval from the [POST 1] for the activation of BCP. • [POST 1] will coordinate with ASD to repair and rebuild the damaged Watson Centre, Kwai Chung and facilities. • After restoration of the affected operations, [POST 2] will seek approval from the [POST 1] for the deactivation of BCP.
Actions to take	• [POST 1] is required to liaise with DMS BEEO system administrator, and other relevant parties to evaluate the impacts to the system and estimate when the operations of DMS BEEO will be restored. • If the anticipated recovery time of the system is longer than the acceptable system down time, [POST 4] should report the current status to [POST 2] and review if the DMS BEEO disaster recovery plan is required to be activated. • If activation is required, [POST 2] should seek approval from the [POST 1] for activation of the disaster recovery plan in Section 7 to setup another system at DR site. • [POST 1] is required to closely monitor the status of the incident and disseminate status update until deactivation of DMS BEEO BCP.

5.2 SCENARIO B : LOSS OF POWER SUPPLY IN EMSD SERVER ROOM

Scenario	Suspension of power supply of server room; or failure of major components of power supply systems in Watson Centre, Kwai Chung leading to stoppage of power supply to server room.
Impact	Unable to provide power supply to server room and the IT equipment in EMSD server room.
Related Parties	[POST 1], [POST 2], [POST 4]
Monitoring, Activation / Deactivation	• Upon receiving any report of power supply failures, [POST 1] is required to closely monitor the incident and determine the impacts to the operations of DMS BEEO. • If [POST 4] finds that the agreed mission-critical activities cannot be performed, [POST 4] should report the situation to [POST 2] and review if BCP of DMS BEEO need to be activated. • [POST 2] will seek approval from the [POST 1] for the activation of BCP. • [POST 1] will liaison with [POST 4] to check if there is any secondary power supply, e.g. UPS, or spare components to replace the damaged one, so as to switch the DMS BEEO operation services to the secondary means and minimise the impact to end users. • After restoration of the affected operations, [POST 2] will seek approval from the [POST 1] for the deactivation of BCP.
Actions to take	• [POST 1] is required to liaise with DMS BEEO system administrator, and other relevant parties to evaluate the impacts to the system and estimate when the operations of DMS BEEO will be restored. • If the anticipated recovery time of the system is longer than the acceptable system down time, [POST 4] should report the current status to [POST 2] and review if the DMS BEEO disaster recovery plan is required to be activated. • If activation is required, [POST 2] should seek approval from the [POST 1] for activation of the disaster recovery plan in Section 7 to restore the DMS BEEO applications at DR site. • [POST 1] is required to closely monitor the status of the incident and disseminate status update until deactivation of DMS BEEO BCP.

5.3 SCENARIO C : DAMAGE AND MALFUNCTIONING OF DMS BEEO SERVERS

Scenario	Hardware broken or malfunctioning to DMS BEEO servers, e.g. Application server, database server, or report server
Impact	Unable to provide services by DMS BEEO system from Watson Centre, Kwai Chung
Related Parties	[POST 1], [POST 2], [POST 4]
Monitoring, Activation / Deactivation	• Upon receiving any report of incidents, [POST 1] is required to closely monitor the incident and determine the impacts to the operations of DMS BEEO. • If [POST 4] finds that the agreed mission-critical activities cannot be performed, [POST 4] should report the situation to [POST 2] and review if BCP of DMS BEEO need to be activated. • [POST 2] will seek approval from the [POST 1] for the activation of BCP. • [POST 1] will coordinate with [POST 2] to assess the extent of damage or malfunctioning of the DMS BEEO Servers, and determine if a replacement is needed to acquire, or contact the corresponding hardware vendor for maintenance. • After restoration of the affected operations, [POST 2] will seek approval from the [POST 1] for the deactivation of BCP.
Actions to take	• [POST 1] is required to liaise with DMS BEEO system administrator, and other relevant parties to evaluate the impacts to the system and estimate when the operations of DMS BEEO will be restored. • If the anticipated recovery time of the system is longer than the acceptable system down time, [POST 4] should report the current status to [POST 2] and review if the DMS BEEO disaster recovery plan is required to be activated. • If activation is required, [POST 1] will also liaison with [POST 2] to restore the DMS BEEO application at the DR site. • [POST 1] is required to closely monitor the status of the incident and disseminate status update until deactivation of DMS BEEO BCP.

5.4 SCENARIO D : SECURITY ATTACKS

Scenario	Various security attacks, e.g. hackers, viruses, unauthorized access, occurred to DMS BEEO
Impact	Unable to perform normal operations by DMS BEEO and provide functionalities to users
Related Parties	[POST 1], [POST 2], [POST 7]
Monitoring, Activation / Deactivation	• Upon receiving any report of the security attacks, [POST 1] is required to closely monitor the incident and determine the impacts to the operations of DMS BEEO. • If [POST 7] identifies and confirms that a security incident has occurred, the reporting and escalation procedure in the "Security Guidelines" should be followed to report and escalate the incidents to [POST 1] and Head of [POST 7]. • [POST 2] will coordinate with [POST 7] to review the firewall policy and strengthen the security measures to stop the loophole. • [POST 2] will seek approval from the [POST 1] for the activation of BCP. • After restoration of the affected operations, [POST 2] will seek approval from the [POST 1] for the deactivation of BCP.
Actions to take	• [POST 1] is required to liaise with EMSD Security Team, [POST 2] and DMS BEEO system administrators, and other relevant parties to evaluate the impacts to the system and estimate when the operations of DMS BEEO will be restored. • [POST 2] is required to liaise with EMSD Security Team to perform necessary eradication actions in the "Security Guidelines" • If the anticipated recovery time of the system is longer than the acceptable system down time, [POST 2] should report the current status to [POST 1] and review if the DMS BEEO disaster recovery plan is required to be activated. • If activation is required, [POST 2] should seek approval from the [POST 1] for activation of the disaster recovery plan in Section 7 to setup another system at DR site and the access to the DR system should be limited within DR site to avoid another security attack. • [POST 1] is required to closely monitor the status of the incident and disseminate status update until deactivation of DMS BEEO BCP.

5.5 SCENARIO E : NETWORK SERVICE FAILURE

Scenario	Network service failure that leads to system down of DMS BEEO
Impact	Affects the availability of DMS BEEO hosted in Watson Centre, Kwai Chung, hence, it affects the normal operations of DMS BEEO users
Related Parties	[POST 1], [POST 2], [POST 5]
Monitoring, Activation / Deactivation	• Upon receiving any report of failures, [POST 1] is required to closely monitor the incident and determine the impacts to the operations of DMS BEEO. • If [POST 5] finds that the agreed mission-critical activities cannot be performed due to network failure, [POST 5] should report the situation to [POST 2] and review if BCP of DMS BEEO need to be activated. • [POST 2] will seek approval from the [POST 1] for the activation of BCP. • [POST 1] will contact [POST 5] to fix the network failure and aim to resume the network service within acceptable system down time. • After restoration of the affected operations, [POST 2] will seek approval from the [POST 1] for the deactivation of BCP.
Actions to take	• [POST 1] is required to liaise with DMS BEEO system administrator, and other relevant parties to evaluate the impacts to the system and estimate when the operations of DMS BEEO will be restored. • If the anticipated recovery time of the system is longer than the acceptable system down time, [POST 2] should report the current status to [POST 1] and review if the DMS BEEO disaster recovery plan is required to be activated. • If activation is required, [POST 1] will also liaison with [POST 2] to restore the DMS BEEO application at the DR site. • [POST 1] is required to closely monitor the status of the incident and disseminate status update until deactivation of DMS BEEO BCP.

6 EMERGENCY CONTACT POINT

In case of system emergency, please refer to the follow parties for emergency contact:

	Name	Post	Email	Contact No.
EMSD				
	-TBC-	--	--	--

6.1 CONTINGENCY MANAGEMENT TEAM (CMT)

6.1.1 Main Duties of CMT

- Activate / deactivate the DR Plan
- Assess the impact of the disaster
- Execute DR Plan
- Monitor and coordinate for the execution of the DR Plan
- Perform DR Drill
- Review and update DR Plan, if required.

6.1.2 Organization of CMT

EMSD CMT is headed by Chief DR Commander and consists of the following members:

Chief DR Commander	[POST 1]
IT DR Commander	[POST 2]
Business DR Commander	[POST 3]
IT System and Software Support	[POST 4]
Computer Operation Support	[POST 4] / [POST 5]
Departmental Administration Support	[POST 6]
End User Support	[POST 6]
EMSD Security Team	[POST 7]
ASD	Government Directory (TBC)

6.1.3 Role and Responsibility of CMT

- Chief DR Commander is responsible to monitor and coordinate all DR activities, to execute DMS BEEO DR Plan, and to manage the operation of the DMS BEEO at DR site.
- IT DR Commander is responsible to assist Chief DR Commander to assess the impact of the disaster, to co-ordinate all DR activities and to execute DMS BEEO DRP on IT aspects, e.g. to recover the system environment and the DMS BEEO at DR site, distribute templates to different units for manual operations during the restoration of the DMS BEEO service in DR site, coordinate IT support to the DMS BEEO and to re-establish the DMS BEEO in production site
- Business DR Commander is responsible to assist Chief DR Commander to assess the impact of the disaster, to co-ordinate all DR activities and to execute DMS BEEO DRP on business aspects, e.g. arrange administrative support including co-ordinate with the administration sections and supplies section for the necessary support service required and coordinate DR users to operate the DMS BEEO.
- IT System and Software Support (EMSD ITMU) is responsible to setting up the system and application software environment of the DMS BEEO at DR site.
- Computer Operation Support (EMSD ITMU) is responsible to provide operation support to the DMS BEEO at DR site, e.g. monitor and re-run the batch jobs of the DMS BEEO,

and perform backup jobs for the DMS BEEO.

- Departmental Administration Support is responsible for administrative support, such as transportation, office and clerical support as well as supply of stationery. EMSD will co-ordinate with the Administration Section and Supplies Section for the necessary support service required.
- End User Support is responsible for co-ordinating all activities of end users during DR.
- ASD is requested to repair/rebuild the damaged computer site. They are co-ordinated by the Chief DR Commander.

7 BUSINESS AND DISASTER RECOVERY DRILL PLAN

7.1 DISASTER RECOVERY (DR) PROCEDURES

7.1.1 Occurrence of a Disaster

A disaster of the DMS BEEO is referred to the circumstance that effectively precludes the provision of the normal computer services for a sustained period of time. Upon the confirmation of disaster occurrence, the Chief DR Commander should be immediately mobilizing an Immediate Response Group to perform an initial assessment on the situation and activate the disaster recovery. The Immediate Response Group would consist of Chief DR Commander, IT DR Commander, Business DR Commander and anyone else required by the situation at that moment in time.

7.1.2 Evaluation of the Impact of a Disaster on Production System

IT DR Commander should assess the impact of the disaster on IT aspects and Business DR Commander should assess the impact of the disaster on business aspects. They should also liaise with other relevant parties to estimate the duration of the outage and when the operations of the DMS BEEO will be restored. They should advise the Chief DR Commander to activate a DR.

An overview outlining a chronological order of typical events and major activities involved in evaluating the impact from a disaster and in triggering the disaster recovery for the system is listed below for reference:

Events	Major Activities	Activity Time (hrs)	Elapse Time (hrs)	Remaining Time (hrs)
Occurrence of an interruption		--	--	72
Investigation and evaluation of impact to the Production System	Investigation and evaluation of the concerned interruption	TBC	TBC	TBC
Activation of Disaster Recovery (DR)	Activate DR Plan	TBC	TBC	TBC
DR System Preparation Procedure	Locate the required hardware	TBC	TBC	TBC
	If backup tapes for system and data recovery are not available, transfer the required backup tapes to DR site	TBC	TBC	TBC
	If hardware devices are not functioning properly, acquire supports from the hardware maintenance vendors	TBC	TBC	TBC

Events	Major Activities	Activity Time (hrs)	Elapse Time (hrs)	Remaining Time (hrs)
DR System Restore Procedure	Prepare DR files for the system recovery from DR backup tapes to a shared storage device and restore the latest backup files from the daily full backup tapes	TBC	TBC	TBC
	Recover the servers (application and database servers) by the DR backup files in the shared storage device	TBC	TBC	TBC
	Modify the server configuration (mapping and changing device drivers of the system s as well as network settings)	TBC	TBC	TBC
	Activate and check the recovered application and database servers	TBC	TBC	TBC
	Redeploy the online application and batch jobs as well as update database	TBC	TBC	TBC
	Check and test the functions of the system	TBC	TBC	TBC

7.1.3 Activation of Disaster Recovery (DR)

Upon a declaration of a DR by the Chief DR Commander, the DMS BEEO DRP will be activated. IT DR Commander and Business DR Commander should notify the DMS BEEO CMT, and other relevant parties the DRP has been activated and start the coordination of all DR activities.

7.1.4 DR System Preparation Procedure

IT DR Commander should coordinate the corresponding parties to locate the required hardware of servers for the recovery of the application and database servers, backup tape drive (tape autoloader), a personal computer for use in the system recovery process, and system full backup tapes for recovering the application, the database, and the data files at DR site for restoring the system environment of the DMS BEEO. If the required devices such as backup tapes or hardware are unavailable at DR site, IT DR Commander should work with Operation Support to check if the required backup tapes or hardware can be transferred from production site to DR site or to acquire the required hardware from hardware maintenance vendors. IT DR Commander should arrange necessary IT support to the DMS BEEO at DR site. The steps are listed below:

	Tasks	Responsible Party	Estimated Time Required
1	Locate the required hardware	IT System and Software Support	TBC
2	If backup tapes (for system and data recovery) are not available, transfer the required backup tapes to DR site	Operation Support	TBC
3	If hardware devices are not functioning properly, acquire supports from the hardware maintenance vendors	IT DR Commander	TBC

Business DR Commander should arrange administrative support including transportation, office and clerical support as well as supply of stationery and other consumables, such as A4 paper and laser printer toner, and co-ordinate with the administration sections and supplies section for the necessary support service required.

7.1.5 DR System Restore Procedure

After the preparation in section 7.2.4 has been completed, the online application and data of the DMS BEEO should be restored at DR site. It was estimated that about 30 hours will be required to complete the restoration and testing on the system. The tasks and the estimated time for each task are listed as follows:

	Tasks	Responsible Party	Estimated Time Required
1	Confirm the availability of computer hardware and the latest full system backup tapes for system recovery in the DR site	IT System and Software Support, Operational Support	TBC
2	Confirm the availability of network connection between the tape autoloader, the application server, and the database server in the DR site	IT System and Software Support, Operational Support	TBC
3	Recover the database server using the daily full backup of the database server	IT System and Software Support	TBC
4	Recover the application server using the daily full backup of the application server	IT System and Software Support	TBC
5	Start up and check the recovered application and database servers	IT System and Software Support	TBC
6	Redeploy the online application and batch jobs as well as update database if necessary	IT System and Software Support	TBC
7	Check and test the functions of the system	IT System and Software Support	TBC

7.1.6 Operation of the Recovered Functions on DR System

Upon the successful recovery of the DMS BEEO at DR site, Business DR Commander should arrange the DR users to operate the DMS BEEO. IT DR Commander should arrange the necessary operational support to monitor the batch jobs, including the daily full backup jobs of the DMS BEEO at DR site, and to re-run these jobs if required.

7.1.7 Backup and Housekeeping Procedures for DR System

The DR system should be scheduled to perform the full system backup process from Monday to Sunday at 3:30am. Two sets with 28 tapes (4 consecutive weeks x 7 days per week) are dedicated to daily full backups from Monday to Sunday. These tapes should be labelled as "DMS BEEO DR <weekday> (Daily) <Week no.>". For example, the tape used on Wednesday in Week 2 and stored in DR Site would be labelled as "DMS BEEO DR Wed (Daily) 2". Two sets of backup tapes will be used in rotation one by one and will be stored at DR site.

7.1.8 Salvage of Computer Centre

Depending on the type of the disaster, the Computer Room and the hardware may have been damaged. IT DR Commander will liaise with the hardware vendors, ASD, to assess the extent of damages, and determine the re-instalment plan.

7.1.9 Re-build Computer Facilities at Department Computer Centre

Business DR Commander will co-ordinate with the computer vendors and seek authorization and funding for the procurement of the necessary equipment for replacement of the damaged equipment, if any, in the EMSD Computer Centre.

If there is any damage to the environmental equipment or other site preparation matters in the Department Computer Centre, which will affect the physical environment for providing computer services. The Chief DR Commander would liaise with Director of Architecture Services and/or Director of Electrical and Mechanical Services for arranging structural and electrical works immediately.

The IT DR Commander will liaise with the computer vendors for the delivery of the installation of the ordered equipment.

7.1.10 Termination of DR

After production site / system of the DMS BEEO has been rebuilt / recovered, IT DR Commander should arrange with IT System and Software Support to restore the latest backup of DR system to

production system. Upon confirmation of the availability of production system, Chief DR Commander will declare the switch-back to production system and formally terminate the DMS BEEO DRP.

7.1.11 DR System Clean-up Procedure

After the switch-back to production system, DR system should be cleaned up by deactivating the corresponding DR servers.

7.2 DR DRILL

7.2.1 Purpose of the DR Drill

The disaster recovery drill should normally be conducted once a year to test the effectiveness of this DRP and to determine what changes may be necessary. Since carrying out a disaster recovery drill could be time-consuming and may affect normal operations, CMT may determine the frequency of conducting drills according to the business environment.

7.2.2 Steps of the DR Drill

CMT should follow the following steps to conduct the DR Drill:

1. Schedule when the DR drill will be conducted and invite DR users to participate the DR drill.
2. Perform DR drill by following the procedures in Section 10.2
3. Log the activities during the DR drill.
4. Review if any changes / improvements on this DRP are required.

7.2.3 Logging of the activities during the DR Drill

During the DR drill, CMT should monitor the progress and record the activities.

7.2.4 DR Drill Review

After DR drill, the CMT should arrange a review meeting with the DR users to review the effectiveness of the DR procedures and identify if any changes / improvements are required.

7.2.5 Update of the DR Procedure Manual

After DR drill review, the DMS BEEO DRP should be updated with the identified changes / improvements and submitted to Chief DR Commander for approval.

8 BACKUP STRATEGY / SCHEDULE / PROCEDURE

8.1 BACKUP MECHANISM

A physical backup server will be assigned for the backup operations for DMS BEEO system. The server will run on Windows Server 2016 and will use Veeam Backup & Replication Enterprise and connect the existing Tape Drive for production DMS BEEO backup.

The backup server will be responsible for the following types of administrative activities:

- Coordinates backup, replication, recovery verification and restore tasks
- Controls job scheduling and resource allocation
- Set up and manage backup infrastructure components as well as specify global settings for the backup infrastructure

The system backup of the servers will be stored in the Backup server and LTO tapes. System backup can be invoked manually when the system configuration is changed. On the other hand, the ESXi Host Server, make use of the Veeam tool to perform scheduled backup. The data is stored into Backup server and LTO tapes.

8.1.1 Backup Jobs Schedule

The backup jobs will be scheduled as below:

Day of Week	Backup Type	Schedule Time	Retention
Monday	Full backup without photos	22:00	7 days
Tuesday	Full backup without photos	22:00	7 days
Wednesday	Full backup without photos	22:00	7 days
Thursday	Full backup without photos	22:00	7 days
Friday	Full backup with photos	22:00	7 days

8.1.2 Backup Files Locations

All the backup files will be stored on the Backup Server, D:\Backup\ in the following folders:

- Production backup : \Backup Job – Production VM\
- UAT backup : \Backup Job – UAT VM\

8.1.3 Backup Tape and Tape Drives

The tape drives for LTO Ultrium is autoloaders. Thus, operating staff is only required to change the set of tapes before the full weekly backup on every Saturday.

The backup tape used by AIX servers system backup should possess the following characteristics:

Format DDS-4 Data Cartridge
Capacity 20 GB or above

The backup tape used by Database Server SSA disk backup should possess the following characteristics:

Format LTO Ultrium Data Cartridge
Capacity 100 GB or above

The backup tape used by Windows 2000 Server backup should possess the following characteristics:

Format AIT Data Cartridge
Capacity 35 GB or above

Backup failure can be caused by either tape drive failure or tape failure. When backup fails, operating staff is requested to report to the support team and clean the tape drive to avoid the possibility of tape drive mal functioning. If the error still occurs, operating staff should test the tape drive with a new tape and replace the damaged tape with a new one. To avoid mal functioning of tape drive, tape drive is recommended to clean monthly.

8.1.4 Labelling of Magnetic Tapes

In general, backup media will be recommended to be labelled to ensure the data to be backed up to the correct tape.

8.1.5 Rotation Scheme

This rotation scheme will be designed to backup data on Weekly basis with 3 weeks retention period.

The following describe the rotation scheme for system backup of Database server:

	Monday	**Tuesday**	**Wednesday**	**Thursday**	**Friday**	**Saturday**
Week 1	BEEODB01 mksysb (Daily) 1	BEEODB01 mksysb (Daily) 2	BEEODB01 mksysb (Daily) 3	BEEODB01 mksysb (Daily) 4	BEEODB01 mksysb (Daily) 5	BEEODB01 mksysb (Weekly) 1
Week 2	BEEODB01 mksysb (Daily) 1	BEEODB01 mksysb (Daily) 2	BEEODB01 mksysb (Daily) 3	BEEODB01 mksysb (Daily) 4	BEEODB01 mksysb (Daily) 5	BEEODB01 mksysb (Weekly) 2
Week 3	BEEODB01 mksysb (Daily) 1	BEEODB01 mksysb (Daily) 2	BEEODB01 mksysb (Daily) 3	BEEODB01 mksysb (Daily) 4	BEEODB01 mksysb (Daily) 5	BEEODB01 mksysb (Weekly) 3

A total of 8 DDS-4 Data Cartridge tapes (5 Daily, 3 Weekly) are required.

8.1.6 Off-site Tape Arrangement

For weekly system backup and weekly SSA disk backup, the backup tape of last week is stored off-site (EMSD operation center). That is, Set 2 tapes will be replaced at the Saturday of next week cycle

by the Set 3 tapes, and that Set 1 tapes will be stored off-site accordingly. Hence, for every moment, there are 2 sets of backup tapes will be stored locally and 1 set will be stored off-site.

For Windows server backup, the backup tapes of the current week is stored off-site, as there are 2 sets of identical backup tapes for a week.

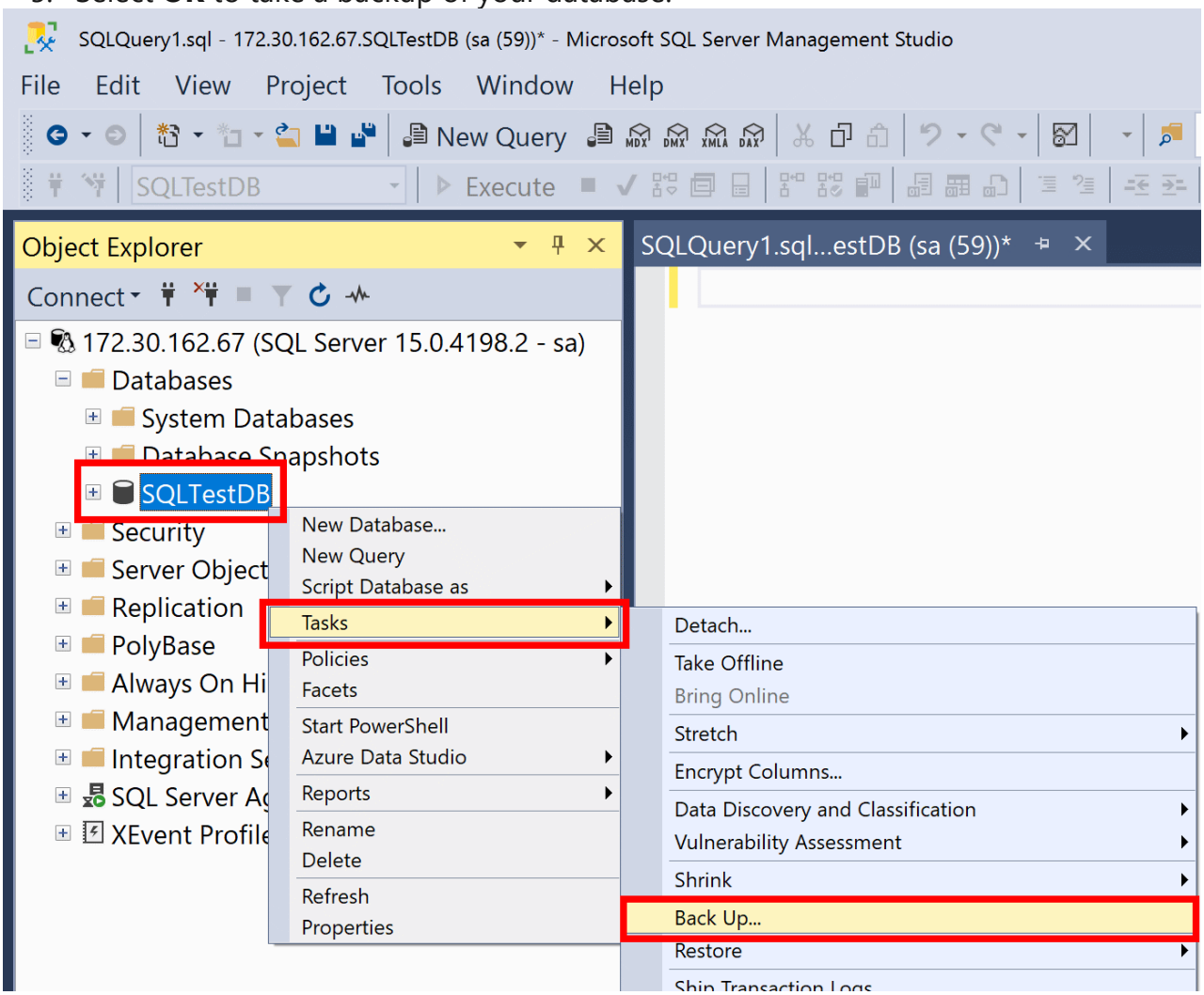
It is suggested to bring the whole set of the weekly tapes to off-site weekly and call back when the set of tapes which are going to be used.

8.2 BACKUP STRATEGY

8.2.1 Database Backup

To take a backup of your database, follow these steps:

1. Launch SQL Server Management Studio (SSMS) and connect to your SQL Server instance.
2. Expand the **Databases** node in **Object Explorer**.
3. Right-click the database, hover over **Tasks**, and select **Back up...**.
4. Under **Destination**, confirm that the path for your backup is correct. If you need to change the path, select **Remove** to remove the existing path, and then **Add** to type in a new path. You can use the ellipses to navigate to a specific file.
5. Select **OK** to take a backup of your database.



8.2.2 Windows / Linux (VM) Servers Backup

Backup of the files stored in Server is scheduled to perform during the non-office hours. backup of files to the LTO tapes. The data is backup into 3 identical set of tapes. One set of tapes are kept on-site while another 2 sets should be kept off-site (Data Centre at EMSD HQ) with the conditions supporting the storage of backup tapes. When necessary, the files can be restored from the any one set of backup tapes to the servers.

The activity log could be checked daily by the following steps:

a) Go to the activity Log.

b) Look for warning messages or error messages to determine the severity and to decide whether it is required to re-run the job.

The job could be re-run by the following steps when necessary:

a) To re-run the job, switch to the windows of "Job Status". Select the job that needs to be re-running, right-click and choose "Reschedule Job".

b) If the error is caused by bad backup media, re-run the backup job using a clean new tape. Then insert the problematic tape and try an ad-hoc backup job for a small number of files. If the media is still with error, try reformatting the tape. If format failed, the tape will not be usable and should be discarded.

c) Modify the date to the previous working date (e.g. if today is 2/10/02, then re-schedule the job to 1/10/02) without changing the time. After pressing OK, the job would start running from the "Job Status" windows automatically. That is no need to re-adjust the schedule after re-running the backup job.

9 TESTING AND VERIFICATION OF BACKUP PROCEDURE

After the backup procedures for DMS BEEO system and database mentioned in Section 8 were performed, there are some measures that can be taken to verify if the backup had been completed successfully and whether the up-to-date data had been backed up.

The ways to test and verify the backup procedure are as follows:

1. Check the backup logs for system and database backup jobs to see if there were any errors during the backup process. If yes, rectification actions need to be taken, and re-run of backup jobs would be needed.
2. For information, the log file of system backup jobs can be found at /backup/log/system_backup.<date>.log
3. For information, the log file of database backup jobs can be found at /backup/log/ BEEO_dr_backup.<data>.log
4. Check the job status for the scheduled jobs on the Backup Server. Job status may either be “READY”, “DONE” or “HOLD”. For the scheduled jobs, make sure the job status is “READY”.
5. Check the job report for the backup jobs on the Backup Server. On the job report, information such as “Type”, “Status”, “Start Date”, “Description” are available to help to spot out any abnormalities for the executed backup jobs.
6. Load the LTO tapes of the full backup performed weekly and extract backup records or image to see if it is up-to-date. Re-run of backup process would be necessary if the backup image was not as expected.

10 RECOVERY STRATEGY / SCHEDULE / PROCEDURE

10.1 RECOVERY STRATEGY

The target recovery time for DR of DMS BEEO would be 72 hours.

10.1.1 DR System Preparation Procedure

- Check if hardware devices listed in section 10.1.2 below are available at DR site
- Check if the hardware devices are functioning properly
- Check if software listed in section 10.1.3 below are installed properly on the DR Servers.
- Check if the latest full backup tapes (for the application and database servers) are available at DR site
- Check if the database, the application server, and the backup tape drive are connected properly through the DR network environment
- Check if the PC computer is functioning properly
- Refer to the DR procedure documents using the PC computer for quick reference

10.1.2 Hardware List for DR

DR AIX Server	
Processor	
CPU	
Operating System	
Memory	
Disk	
Disk Storage	
Disk Storage Total	

10.1.3 Software List for DR

Server Role	**Software Particulars**
Database Server	

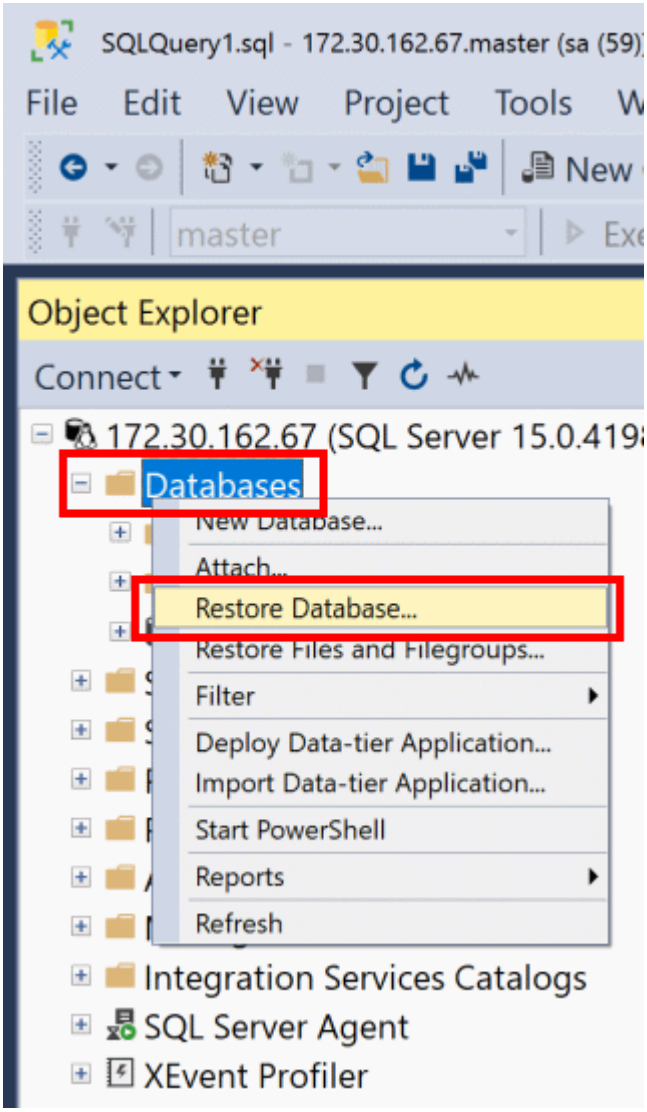
Server Role	Software Particulars
Web/Application Server	
Report Server	
Image Server	
GIS Server	

10.2 RECOVERY PROCEDURE

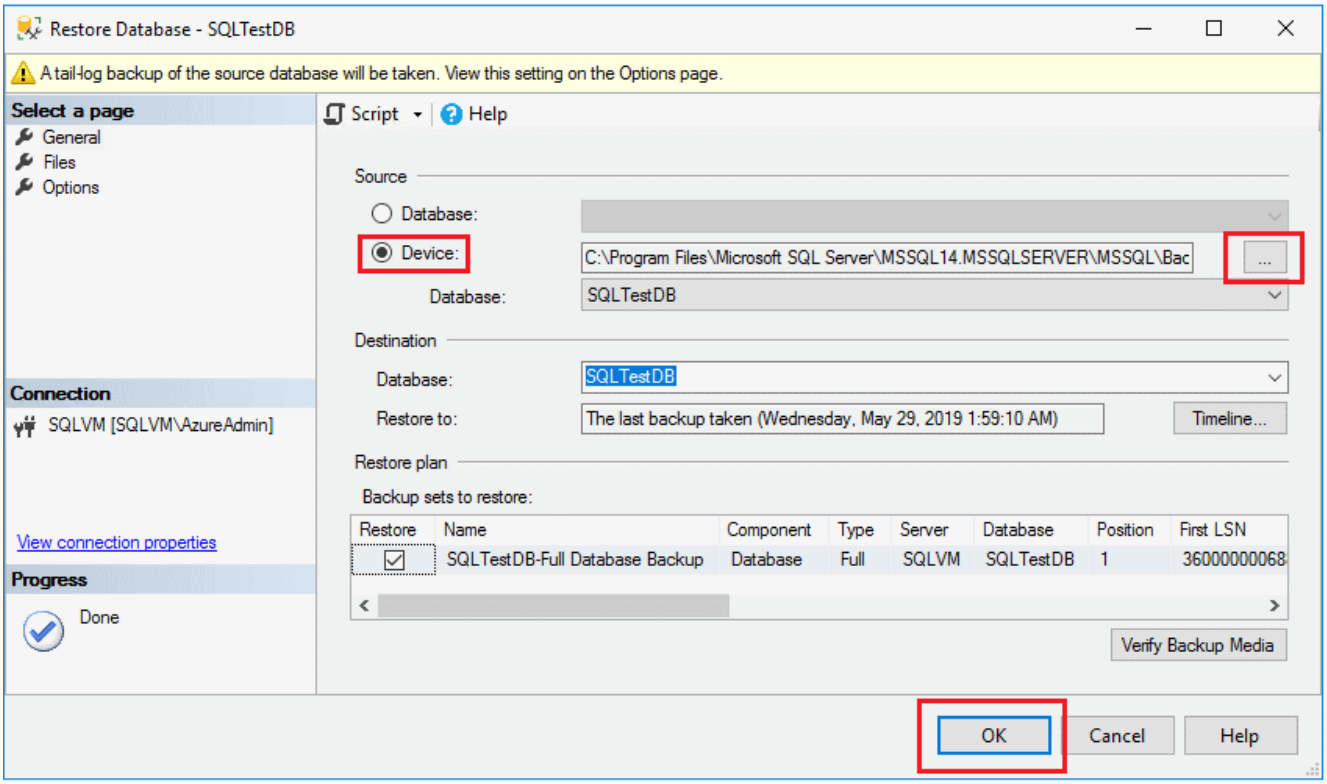
10.2.1 Database Server Restore

To restore your database, follow these steps:

1. Launch SQL Server Management Studio (SSMS) and connect to your SQL Server instance.
2. Right-click the **Databases** node in **Object Explorer** and select **Restore Database...**.



3. Select **Device:**, and then select the ellipses (...) to locate your backup file.
4. Select **Add** and navigate to where your `.bak` file is located. Select the `.bak` file and then select **OK**.
5. Select **OK** to close the **Select backup devices** dialog box.
6. Select **OK** to restore the backup of your database.



10.2.2 Windows Servers Restore

There are 8 slots in the autoloader and a tape drive in the LTO tape unit. Please follow the steps below to load/replace tapes to LTO tape unit:

a) Please make sure that no backup is processing when change the tapes.

b) You can control the movement of the tapes by the control buttons on LTO

c) If there is tape inside the drive, please move that tape back to the autoloader, by press the Menu button, then Move Tape, and choose the slot number to move the tape from the drive.

d) Press the Menu button, and choose Eject/Insert Tapes.

e) Choose multiple mode, and then press enter to start replacing the tapes.

f) The autoloader will then move from slot 01 to slot 07. For each slot, take out the old tape and insert a blank tape.

g) Slot 08 is the cleaning tape. Hence there is no need to replace it.

h) Label the old tapes with appropriate slot number and description such as the date of backup.

i) Wait about 20 minutes for the LTO to recognize the tape, then format or erase the tapes, following the steps mentioned above.

11 TESTING AND VERIFICATION OF RECOVERY PROCEDURE

After DMS BEEO system and database was restored according to the procedures mentioned in Section 10, there are some measures that can be taken to verify if the restore had been completed successfully and whether the correct set of data had been resumed.

The ways to test and verify the restore procedure are as follows:

1. Login to DMS BEEO database and perform sql query for tables used by major functions to check if the record's last updated date match with the backup date of the restored database.
2. Login to the restored DMS BEEO system and perform query for major functions, such as FN-LEF-008 "Form LE5 – Current Application (Lift/Escalator)", FN-CON-003 "Contractor Registration – Current Application", or FN-DMS-001 "View Document", to check if the records/documents could be loaded properly and the corresponding information are matching with the backup date of the resumed image.
3. Check the "Activity Log" of the restore process to see if the job had been completed successfully or not. If not, the restore process would need to be re-run.

12 BACKUP JOB AND CONFIGURATION

The backup jobs and its schedules are depicted as below:

Backup job	Schedule	Schedule Start Time	Schedule End Time
DB server	Daily & Weekly System Backup	11:30pm	12:00pm

13 APPENDIX

N/A

- End of Document -