Backup & Recovery Procedure

Sign Off

	Name, Title, Department	Signature	Date
Prepared by	Ricky Ng (DoIT, IT Division)		Sept-Oct 2024
Reviewed by	Deputy Chief Executive		Oct 2024
Approved by	Full Council		11 Dec 2024

This procedure is owned by Information Technology Division and established to satisfy Backup & Recovery Standard. Any changes and/or adjustments to this procedure should be made, reviewed, and approved by Information Technology Division.

Consumer Council Document Library Access Right

Access Party
All Users of Consumer Council

Revision History

Version Date	Version Number	Description of changes	Author
11 Dec 2024	1.0	N/A	Protiviti / ITD
30 Jun 2025	1.1	General • Change of Titles: Updated all references from “Division Head” to “Director”. • Renaming of OGCIO: Changed all references from “OGCIO” to “DPO”. • Renaming of AGDEIT: Changed all references from “AGDEIT” to “Committee on Digital Economy and Information Technology (DEIT)”.	Protiviti / ITD

Table of Contents

1 Scope

This procedure is to provide a high-level framework to relevant staff and relevant parties in support of managing IT Systems backup and Recovery. Detailed procedures and technical contents of the resolution, if required, should be incorporated into the procedures of individual supporting teams.

This procedure should be read in conjunction of Backup & Recovery Standard.

2 Statement of Responsibility

2.1 The statement of responsibility should reference Backup & Recovery Standard.

3 Backup Schedule

3.1 The backup schedule outlines the frequency and timing of various backup operations, including daily, weekly, monthly, or other periodic backups.

3.2 The backup schedule should be defined as shown below:

System Name	Description	Backup Frequency	Offline Offsite Archive	Destroy After
IT internal System	Active Directory, ITSR, Print Server etc.	Every Night	Weekly	1 Year
HR System	HR System	Every Night	Weekly	1 Year
Accounting System	Accounting system	Every Night	Weekly	1 Year
Online Price Watch	Online Price Watch	Every Night	Weekly	1 Year
Application Public website	Application Public website	Every Night	Weekly	1 Year
ODR & CCMS 2.0	ODR & CCMS 2.0	Every Night	Weekly	1 Year
IVRS	IVRS	Every Night	Weekly	1 Year
Online Booking	Online Booking	Every Night	Weekly	1 Year

System	System			

4 Backup Methodology

4.1 The Backup methodology outlines the methods to be used for the backup of the IT systems. The following methodologies are designed to ensure data protection while allowing efficient recovery of data loss or corruption.

4.2 Types of Backups

4.2.1 Full Backup: A complete copy of all selected data is made, providing a single point-in-time snapshot that can be used to restore the system.

4.2.2 Incremental Backup: Only the changes made since the last backup (full or incremental) are copied.

4.3 Backup Format

4.3.1 Image-based Backup: This method takes a complete snapshot of a system image, including the OS, applications, settings, and files. It is ideal for rapid restoration of entire system to a specific state.

4.4 Encryption and Security

4.4.1 All backup data must be encrypted using industry-standard encryption protocols. Access control measures must be implemented to ensure only authorized personnel can access backup files.

5 Backup Monitoring

5.1 The backup logs should be created electronically by the backup software and reviewed daily IT Technical Manager to ensure timely resolution of failed job events.

5.2 The daily backup job report should record all successful and failed backups.

5.3 The failed backup jobs must be reported in the ITSR system to document the backup incident. For the incident handling procedure, please refer to Incident Management Procedure.

6 Restoration

6.1 The restoration requests shall be submitted to ITSR with legitimate business justification (e.g. data loss, disaster recovery), and reviewed and approved by Director of IT, Director of the user division concerned and IT Security Manager.

6.2 IT Division should contact the user to evaluate and confirm the integrity of the restored data and test the restored system to ensure functionality before going into production.

7 Backup Restoration Testing

7.1 The backup restoration testing for Critical Business Service and Core Business Service should be performed at least annually by IT Technical Manager to determine if the systems can be restored successfully.

7.2 The IT Technical Manager, IT Security Manager, and Director of IT should review the backup restoration test result. Issues from restoration tests shall be reported in the ITSR system. For the issue-handling procedure, please refer to the Incident Management Standard and Change Management Standard.

8 Disposal Backup Tapes and Hard disks

8.1 Disposal of backup tapes and hard disks must be handled by approved vendors and must be updated on the IT inventory list.

8.2 The disposed backup tapes and hard disks shall be physically destroyed or degaussed by approved vendors.

9 Exemption

9.1 For situation arise where it is not possible to comply with the guideline requirements, formal approval should be obtained from the Director of IT or delegate(s).

9.2 All exceptions should be protected by sufficient alternative security controls or process to enforce the security and compliance.

10 Related Policy and Procedural Documentation

- IT Security Policy
- Password Policy
- Endpoint Security Standard
- Identity and Access Management Standard
- Log and Event Management Standard
- Vulnerability and Patch Management Standard