消費者委員會
CONSUMER COUNCIL

Backup and Recovery Standard

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 standard is owned by Information Technology Division and established to satisfy the IT Security Policy. Any changes and/or adjustments to this standard 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 standard applies to all data collected and processed in the Consumer Council IT systems. The IT systems include all information systems managed or outsourced by the Consumer Council, including servers, workstations and applications.

2 Statement of Responsibility

Business Owner (Director)

2.1 Director, who is the owner of the systems, shall be responsible for ensuring all the backup and recovery requirements are provided to IT Technical Manager for implementing the backup plan to meet recovery time objectives (RTO) and recovery point objectives (RPO) of the systems.

2.2 Director shall be responsible for confirming data backup requirements, scopes, and schedules.

2.3 Director shall be responsible for informing IT Technical Manager and IT Security Manager after any change on business requirement.

IT Technical Manager

2.4 IT Technical Manager shall be responsible for developing and implementing backup plans including the data backup and restoration requirements, scopes, and schedules to meet the RTO and RPO requirements.

2.5 IT Technical Manager shall be responsible for monitoring the status of backup and recovery tasks, and performing actions when issue/failure is notified.

2.6 IT Technical Manager shall be responsible for ensuring that all in-scope IT systems are backed up and restored within the defined backup and restoration requirements.

IT Security Manager

2.7 IT Security Manager is responsible for ensuring backup data is sufficiently protected.

2.8 IT Security Manager is responsible for ensuring the security of Consumer Council IT environment during recovery processes.

Director of IT

2.9 Director of IT is responsible for ensuring the Consumer Council's data integrity and availability by developing and implementing the backup and recovery policy and procedure.

3 Data Backup

3.1 Recovery time objectives (RTO) and recovery point objectives (RPO) must be established and documented for all IT systems to ensure it is aligned to their business resumption and system recovery priorities.

3.2 Technical and procedural controls shall be established and maintained to manage the Consumer Council's IT system availability and recoverability. IT systems shall be designed and implemented to achieve the level of system availability that is commensurate with its business needs.

3.3 Backups shall be conducted at regular intervals. Backup plan and schedule for IT systems shall be established and approved by the Director of IT, Director of which he/she is the business owner of the system, and IT Security Manager.

3.4 Backup activities shall be performed according to the approved backup plan.

3.5 System full backup shall be conducted at least annually.

3.6 The changes in backup requirements, scopes and schedules shall be approved by the Director and IT Security Manager.

4 Backup Monitoring

4.1 Backup status shall be monitored and documented regularly based on backup schedules.

4.2 Records for failed backup jobs and backup task re-execution shall be documented after investigation. For repeatedly failed backup tasks (e.g. 3 successive times) that cannot be resolved, the issue shall be reported as an incident according to Incident Management Standard.

5 Backup Storage

5.1 Offline off-site backup shall be performed to avoid inadvertent loss or corruption of all data when the Council's systems are compromised.

5.2 Only authorized users shall have access to backup data to ensure its confidentiality and integrity.

5.3 Security measures, with level of security on par with production and operational data, shall be implemented to protect the backup data when stored.

5.4 Backup data must be encrypted by following the cryptography standard in IT Secuity Policy and fulfill the security requirements in Information Classification and Protection

Standard.

5.5 Backup media shall be locked in a secured area to prevent unauthorized access.

5.6 Backup media (e.g. back tapes) must be encrypted and secured when being transported between the backup storage location and off-site storage location.

5.7 Logs shall be maintained for the transportation of backup tapes.

5.8 Retention period for backup data must comply with the data retention requirements referencing Information Classification and Protection Standard.

5.9 Retired backup media (e.g. back tapes and disks) shall be reviewed and disposed regularly after the expiry of the data retention period.

6 Data Recovery

6.1 Restoration shall only be performed with legitimate business justification (e.g. data loss, disaster recovery), and the restoration request shall be reviewed and approved by Director of IT, Division Director and IT Security Manager.

6.2 The IT Technical Manager shall be responsible for performing the data restoration based on requests approved in accordance with section 6.1 above.

6.3 Validation must be performed after data successfully recovered to ensure the integrity and completeness, and results shall be reviewed and approved by Director of IT, Director and IT Security Manager. Follow-up must be performed if there is any issue noted.

6.4 Backup data restoration test must be performed at least annually to ensure the backup and recovery are well performed and available for emergence cases, including disaster recovery, ad-hoc database restoration, and dedicated file restoration.

6.5 The IT Technical Manager shall be responsible for ensuring the completion of data restoration tests, and the test results shall be reviewed by IT Technical Manager, IT Security Manager and Director of IT. Issues from restoration tests shall be followed up.

7 Exemption

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

7.2 All exceptions shall be protected by sufficient alternative security controls or processes to enforce the security and compliance.

8 Related Policy and Procedural Documentation

- Backup and Recovery Procedure
- Incident Management Standard
- Information Classification and Protection Standard

9 Related Reference(s)

The standard is developed with reference to the following document(s):

- DPO S17 Baseline IT Security Policy
- DPO G3 IT Security Guidelines