CITY UNIVERSITY OF HONG KONG
Business Continuity Management Standard

(Approved by the Information Strategy and Governance Committee in January 2023)

Document Control

Document Owner	Classification	Publication Date
CSC	PUBLIC	2023-01-28

Revision History

Version	Date	Summary of Changes
1.0	2013-12-19	Initial Release
1.1	2015-08-24	Typo corrections Removed reference to “Business Continuity Plan for IT Systems”, of which privilege to access by general staff was revoked.
1.2	2023-01-28	Revised the link in this document.

Distribution

Copy	Issued to	Location
Master	Public	https://www.cityu.edu.hk/csc/information-security/information-security-policies-and-standards

Contents

1 Policy Statement

The City University of Hong Kong ("University") shall take all reasonable steps to ensure that in the event of a service interruption, essential operations will be maintained and normal services will be restored as soon as possible.

The University shall also have documented, tested and regularly reviewed Business Continuity Plans ("BCP") which describe how business will be conducted if critical Information Systems are disrupted.

2 Roles and Responsibilities

2.1 Management of the University

Management of all University Units shall establish and manage a process for developing, implementing and maintaining business continuity for critical information processing facilities, business operations, and IT services under their control.

2.2 University Units

The University Units which are responsible for the business operations are also responsible for the identification of their critical businesses and the development of corresponding BCP(s) in event of information systems disruptions.

The University Units shall appoint BCP Team Leader and Members, and defined their roles and responsibilities during and following an incident, e.g. primary and deputy coordinators responsible for notifying the affected stakeholders.

2.3 Information System Owners

Owners of information systems shall identify availability and business continuity requirements in business plans and contractual requirements, service level agreements and risk assessments, which shall be reviewed and monitored regularly.

The supplement process and availability management shall also be established to ensure the appropriate deployment of resources, methods and techniques, and to support the availability of information system services agreed with users.

2.4 Crisis Management Team ("CMT")

A Crisis Management Team ("CMT") is an administrative and decision-making body that is responsible for coordinating of BCP in the event of a disaster.

The senior management of the University shall setup a University level CMT, which consists of senior management members from all key University Units. The University level CMT is activated by the Chief Information Officer ("CIO").

The management of University Units and research centers shall setup Departmental CMT for their mission critical Information systems and services.

The University level CMT and departmental CMT are responsible for:

- Examining and assessing the impact of the failure of information systems and services under their control
- Assessing and deciding on whether or not to activate Business Continuity Plan(s)
- Assessing and deciding on whether or not to resume operations from the original location
- Communicating and coordinating with relevant internal and external constituencies during the implementation of the BCPs
- Managing the business recovery and resumption efforts
- Making public announcements when necessary

3 Business Impact Analysis and Risks Assessment

The management of the University shall analyze the activities in the University and determines the continuity and recovery priorities, objectives and targets. The University shall also identify, assess and manage the risk of disruptive incidents.

The business impact analysis shall:

- Evaluate the impacts over time of not performing these activities
- Identify dependencies and supporting resources and stakeholders for these activities

At minimum, the following actions shall be taken by the University as part of the risk assessment practice.

Action	Action Description
Key Process Identification	• Identify mission critical processes and their supporting activities
Impact Analysis	• Identify the impacts resulting from interruption, disruption, non-availability and disaster scenarios • Identify priority and timeframes for resuming these activities, the recovery time objective and Maximum Tolerable Period of Disruption ("MTPD")
Risk assessment	• Identify the risk of disruption to the University's prioritized activities and the processes, systems, information, people, assets, partners and other resources supporting them • Identify treatments commensurate with business continuity objectives
Select business continuity strategy	• Determinate appropriate strategy for protecting prioritized activities • Establish resource requirements to implement selected strategies

4 Design and Implement Business Continuity Management

The University shall, at minimum, consider the following aspects when designing business continuity management procedures and compilation of BCP.

4.1 Business Recovery Procedure

A recovery procedure shall be defined to briefly describe the sequence and the level of services to be recovered in the events of service interruption. The recovery checklist should contain the steps to be followed during the crisis. The following information must be clearly specified for each step:

- Responsible personnel that execute the steps
- Duration of the steps to be completed
- Next steps under different circumstances and corresponding fall back procedures
- Backup staff resource in case the responsible personnel are unavailable

The recovery procedures should be adequately documented, distributed to relevant parties and regularly reviewed for relevancy.

4.2 Maximum Tolerable Period of Disruption ("MTPD") and Recovery Time Objective ("RTO")

MTPD is the time it would take for adverse impacts to become unacceptable, if certain operations or functions cannot be provided after a failure or disaster occurs.

RTO is the period of time following an incident within which the process must be resumed. The RTO has to be less than the MTPD.

Each academic or administrative unit shall determine its own minimum level of service required to sustain the normal operations and corresponding MTPD and RTO.

4.3 Presuppositions and Dependencies

Presuppositions or dependencies in relation to the execution of steps in recovery procedures and to the achievement of specific RTOs should be identified by each unit within the University. For example, during the month/year end close of the University's financial statement, the ledger system should be resumed for operation within 8 hours. During the rest of the time, the ledger system should be resumed within 24 hours.

In addition, all these presuppositions and dependencies must be documented in the BCP together with the respective recovery procedures and RTOs.

4.4 Composition of BCP

The following components must be included in the BCP of the University:

- CMT members and reporting hierarchy
- BCP Team Leaders and Members
- Contact and/or Emergency contact of all involved persons
- Location of backup operation premises
- Secondary telecommunication architecture
- Recovery procedures and relevant presuppositions or dependencies
- RTOs and relevant presuppositions or dependencies

5 Testing

The University Units shall ensure that their BCP(s) are tested internally or cross units, if there are dependencies among the business of the units, at least annually or when any significant change has occurred to the University's operational or IT environments.

The University shall ensure that all components of the BCP are verified and all relevant parties participate during the testing.

The BCP test should be scheduled at a time when it minimally impacts the University's normal operations, services, staff, students or any relevant third parties.

The University shall monitor the BCP test results at the time that the testing plan is drawn up and compare to the expected results (e.g. RTOs). Any failed components should be investigated and necessary updates should be made to meet the expectation.

The BCP test results should be documented and retained for at least 12 months or after the revision of BCP is completed, whichever is later.

6 Training

The management of the University shall organize regular training on business continuity awareness for its members, including staff and students (if possible) at least on an annual basis. Attendance records should be retained and monitored to ensure that all members of the University participate in the training program.

For staff and students that are not involved in business continuity awareness training, clear guidelines (e.g. notifications, signage and instructions), shall be provided to them during a service interruption.

The University shall establish on-going promotion and communication of overall business continuity management policy and BCP to its staff, students or any relevant third parties to ensure that the policies and plans are understood, implemented and achieved.

7 Distribution and Maintenance

7.1 Distribution

The BCP documentation should be distributed to the following members of parties in both softcopy and hardcopy form:

- CMT members
- BCP members
- Help Desk Service of CSC and any other departmental service support staff

A copy of BCP documentation should be stored offsite in a secured manner to ensure that the plan can be implemented when the primary premises of the University is unavailable.

7.2 Maintenance

Appropriate adjustment to the BCP shall be made under the following circumstances:

- When there are changes to the University's activities, such as new key process, obsolete operational procedures, relocation of facilities and resources, and changes in legislation guidance.

- When there are changes in objectives and strategy of the University
- When there are deficiencies identified during the BCP test, which require amendment or re-design of respective BCP components. For example, certain recovery procedures cannot be correctly performed due to additional dependencies.
- When there are changes to CMT members, BCP members and reporting hierarchy
- When there are changes to backup operation premises and secondary telecommunication architecture

The University shall ensure that any updates to the BCP are reviewed by management of respective University Units. The updated BCP should also be distributed to all relevant parties timely.

7.3 Reporting

Yearly BCM reporting shall be undertaken through all levels of the University to track the maintenance status of BCP. The University shall ensure that all University Units acknowledge the correctness of the BCP in relation to their operational areas.

8 Summary

The University shall implement business continuity management to ensure its core operations continue to perform in a controlled manner during service interruptions. An up-to-date and well tested BCP should be maintained to drive the switch-over procedures from normal to emergency operational mode and vice versa.