Appendix L

DISASTER RECOVERY AND CONTINGENCY PLANNING CHECKLIST FOR ICT SYSTEMS

I. GETTING READY

☐ **A.** Obtain written commitment from top management of support for contingency planning objectives.

☐ **B.** Assemble the contingency planning team to include one or more permanent members from:

1. Computer support staff
2. Operational or unit managers
3. Facilities management
4. Department Safety Committee
5. ICTSO

☐ **C.** Provide for the planning committee to include participation on an "as needed" basis from the following departments:

1. Internal Audit (compliance)
2. Police (coordination)
3. Information & Communications Technology (ICT)
4. Others as required.

☐ **D.** Define the responsibility of planning committee members. Appoint;

1. Moderator to facilitate planning meetings
2. Secretary to take and prepare meeting notes and agenda's
3. Administrator to aggregate meeting materials

II. GATHERING NECESSARY INFORMATION - RISK ASSESSMENT

☐ **A.** Prepare a written description of the mission - critical functions of the Department and Units.

☐ **B.** Identify the areas impacted by an emergency:

1. Functional Operation of the Department
2. Service to Clients/ Staff
3. Obligations to Vendors/ Suppliers/ Agencies
4. Relations with Other Departments
5. Department Credibility
6. Other Departmental Impacts

☐ **C.** Define and establish estimated potential losses and liability to the department due to lost or delayed functions, in order of severity of the emergency:

Severity	Amount or range (RM)	Duration
1. Catastrophic	_____	_____
2. Major	_____	_____
3. Serious	_____	_____
4. Limited	_____	_____

☐ **D.** Determine which critical department functions depend on ICT systems. List critical functions with the associated ICT system(s). Contingency planning for critical functions beyond their information systems components should be referred to the department recovery planning effort.

☐ **E.** Establish the vulnerability of ICT systems by examining possible consequences and frequency of specific emergencies.

Specific Emergencies	Possible Consequences
1. Earthquake	1. Prohibited Access
2. Fire	2. Disrupted Power
3. Flood	3. Power Outage
4. Landslide	4. Water Damage
5. Bomb/ Explosion	5. Smoke Damage
6. Sabotage	6. Chemical Damage
7. Power Failure/ surge	7. Structural Damage
8. Other?	8. Communication loss
	9. Other?

☐ **F.** Using the information in **A through E** make a prioritized list of mission critical ICT system functions for restoration in an emergency.

III. GATHERING NECESSARY INFORMATION - RESOURCE ASSESSMENT

☐ **A.** Survey the systems and data which are critical to the Department's functions. Develop flow charts of the results. Verify flow diagrams with appropriate system administrator. The survey should ascertain:

1. Source of all data used in the system
2. Nature of information or report
3. Frequency of need for data
4. How the data is obtained, paper, e-mail, remote access download, tape or disk.
5. Who in department receives or retrieves data.

6. Who on the department do you speak to about access to the data? Will they be available in an emergency?
7. What is the impact if this data is not available
8. Hardware/ OS software
9. Network.
10. Applications.

☐ **B.** Determine if the current backup plan is adequate for the completed risk assessment and includes the following features:

1. Routine periodic backups,
2. Clear backup “strategy” (full vs. incremental backups, frequency, etc.),
3. Off-site storage and retrieval procedures,
4. Alternate processing site (hot, warm, or cold site)

☐ **C.** Complete a resource inventory in each of the following areas (items that might have to be replaced):

1. Equipment
   a. Computer hardware
   b. Network hardware
   c. Other equipment
2. Documentation
   a. Procedure manuals/ handbooks
   b. Software
   c. Accounting procedures
   d. Communication documentation
3. Others

☐ **D.** Define the responsibilities of emergency response team(s).

☐ **E.** Complete staff responsibility chart for emergency response.

1. Disaster evaluation team (management level)
2. Interim operations team
3. Recovery team

IV. INTEGRATION WITH DEPARTMENT RESPONSE AND RECOVERY PLANNING

☐ **A.** Specify who is authorized to declare a disaster and activate the information systems emergency Plan.

☐ **B.** Define the department's immediate response actions by referring to the Department Safety Plan for evacuation and notification of staff.

1. Accounting for staff and others in the building.
2. Meeting location of disaster evaluation team.
3. Reaching staff needed for emergency response.
    a. List of home telephone numbers
    b. Cellular phone

☐ **C.** The Department Recovery Plan should define "manual" processes that can be used until ICT resources are recovered. This need for parallel paper process is beyond the planning scope of information system group. It needs to be defined by a department administrative recovery team. This plan should:

1. Stock the required forms.
2. Pre-assign batch numbers, queue numbers, work order numbers, service request numbers, etc.
3. Document procedures to merge the manually tracked data with the information on the system once it is restored.
4. Prescribe how the impact of changes in procedures will be clear to customers, vendors, etc.

V. INTERIM OPERATION PLAN - PREARRANGED AGREEMENTS FOR RESOURCE REPLACEMENT

☐ **A.** Possibilities for alternate site:

1. Other department with similar facilities
2. Other department in the immediate geographical area
3. Computer manufacturer's facilities (or other suggestions from them)
4. Service bureaus in the immediate area

☐ **B.** Considerations for alternate site selection:

1. Building type
2. Floor capacity - space and load
3. Raised flooring
4. Electric circuits/ capacity/ special connectors
5. Air conditioning and humidity control
6. Chilled water
7. Fire protection and suppression
8. Security - personnel
9. Security - physical
10. Security - data
11. Communications
    a. Telephones.
    b. Network between departmental systems and access to other data.
    c. Physical access to systems with critical data which are not accessible remotely.

☐ **C.** Back-up agreements:

1. Written guarantee or contract with other companies.
2. Reciprocal agreements
3. Service bureau commitments
4. Vendor commitments

☐ **D.** Alternate hardware:

1. Computer and components
   a. CPU model
   b. Memory
   c. Operating system
   d. Options
   e. Peripherals
2. Network equipment and wiring
3. Terminals
4. Off-line equipment
5. Furniture
6. Office machines (including phones, fax, etc.)

☐ **E.** Supplies:

1. Paper
2. Forms
3. Disks
4. Tapes
   a. Reel
   b. Cartridge (type)

☐ **F.** Off-site moving plans:

1. Transportation of staff
2. Transportation of data and supplies
3. Staff phone list
4. Other _____

VI. TEST, EVALUATE AND UPDATE THE PLAN

☐ **A.** Specify periodic testing of the contingency plan to assure processing compatibility:

1. Frequency
2. Scope
3. Test data
4. Test evaluation team

☐ **B.** Periodically review and update of emergency response documentation:

1. Staff responsibility charts
2. Staff telephone numbers
3. Vendors
4. Software license agreements
5. Alternate site agreements
6. Inventory of computer hardware and software
7. Interim operations procedures

☐ **C.** Periodically review and drill emergency response and recovery teams:

1. Tabletop exercise to test documentation and communication in controlled environment.
2. Functional exercise to test documentation, communication and procedures in controlled environment.
3. Field exercise to test documentation, communication, procedures and logistics in a simulated “real” environment.

VII. RECOVERY AND RESTORATION

☐ **A.** Permanent site preparation:

1. Building
2. Floor capacity - space and load
3. Raised flooring
4. Electric circuits/ capacity/ special connectors
5. Air conditioning and humidity control
6. Chilled water
7. Fire protection and suppression
8. Security - staff
9. Security - physical
10. Security - data
11. Communications
    a. Telephones
    b. Network between departmental systems and access to other data
    c. Physical access to systems with critical data which are not accessible remotely.

☐ **B.** Procurement of hardware:

1. Acquisition
2. Computer and components
    a. CPU model
    b. Memory
    c. Operating system
    d. Options
    e. Peripherals

3. Network equipment and wiring
4. Terminals
5. Off-line equipment
6. Furniture
7. Office machines (including phones, fax, etc.)

☐ **C.** Supplies:

1. Paper
2. Forms
3. Disks
4. Tapes
   a. Reel
   b. Cartridge (type)

☐ **D.** Parallel operations plans.

☐ **E.** Migration plan

☐ **F.** Procedures to close down the interim operation