Sample IT Continuity Plan Template

V 1.0

Steve Taylor, Information Security Manager

(based on NIST Special Publication 800-34)

This sample format provides a template for preparing an information technology (IT) Continuity plan. The template is intended to be used as a guide and the faculty or PAC IT Continuity Planning Coordinator should modify the format as necessary to meet their local system's IT Continuity requirements and comply with any faculty or PAC internal policies.

Where practical, the guide provides instructions for completing specific sections. Text is added in certain sections; however, this information is intended only to suggest the type of information that may be found in that section. The text is not comprehensive and should be modified to meet specific faculty or PAC requirements and system considerations.

The IT Continuity plan should be marked with the appropriate security label, such as *Internal Use Only*.

1. INTRODUCTION

1.1 PURPOSE

This {system name} IT Continuity Plan establishes procedures to recover the {system name} following a disruption. The following objectives have been established for this plan:

- Maximize the effectiveness of IT Continuity operations through an established plan that consists of the following phases:
  - **Notification/Activation phase** to detect and assess damage and to activate the plan
  - **Recovery phase** to provide temporary IT operations and recover damage done to the original system
  - **Restoration phase** to restore IT system processing capabilities to normal operations.
- Identify the activities, resources, and procedures needed to carry out {system name} processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated {faculty or PAC name} personnel and provide guidance for recovering {system name} during prolonged periods of interruption to normal operations.
- Ensure coordination with other {faculty or PAC name} staff who will participate in the IT Continuity planning strategies.
- Ensure coordination with external points of contact and vendors who will participate in the IT Continuity planning strategies.

1.2 APPLICABILITY

The {system name} IT Continuity Plan applies to the functions, operations, and resources necessary to restore and resume {faculty or PAC name}'s {system name} operations as it is installed at {primary location name}. The {system name} IT Continuity Plan applies to {faculty or PAC name} and all other persons associated with {system name} as identified under Section 2.3, RESPONSIBILITIES.

1.3 SCOPE

Planning Principles

Various scenarios were considered to form a basis for the plan, and multiple assumptions were made. The applicability of the plan is predicated on two key principles;

- The {faculty or PAC name}'s facility in {location} is inaccessible; therefore, {Organization name} is unable to perform {system name} processing for the {faculty or PAC name}.
- A valid contract exists with the alternate site that designates that site {location} as the {faculty or PAC name}'s alternate operating facility.
  - {faculty or PAC name} will use the alternate site building and IT resources to recover {system name} functionality during an emergency situation that prevents access to the original facility.
  - The designated computer system at the alternate site has been configured to begin processing {system name} information.

- The alternate site will be used to continue {system name} recovery and processing throughout the period of disruption, until the return to normal operations.

Assumptions

Based on these principles, the following assumptions were used when developing the IT Continuity Plan;

- The {system name} is inoperable at the {faculty or PAC name} computer facility and cannot be recovered within 48 hours.
- Key {system name} personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the {system name} IT Continuity Plan.
- Preventive controls (e.g. generators, environmental controls, waterproof covers, sprinkler systems, fire extinguishers, and fire service assistance) are fully operational at the time of the disaster.
- Computer equipment, including components supporting {system name}, are connected to an uninterruptible power supply (UPS) that provides 45 minutes to 1 hour of electricity during a power failure.
- {system name} hardware and software at the {faculty or PAC name} original site are unavailable for at least 48 hours.
- Current backups of the application software and data are intact and available at the offsite storage facility at {location}.
- The equipment, connections, and capabilities required to operate {system name} are available at the alternate site in {location}.
- Service agreements are maintained with {system name} hardware, software, and communications providers to support the emergency system recovery.

The {system name} IT Continuity Plan does not apply to the following situations:

- **Overall recovery and continuity of business operations**. The UoA Business Continuity Management Plan fulfils this function.
- **Emergency evacuation of personnel**. The Emergency Evacuation Plan (EEP) is {enter details}
- {Add any additional constraints to this list}

1.4 REFERENCES/REQUIREMENTS

This {system name} IT Continuity Plan complies with The University of Auckland's *IT Continuity and DR Planning Policy* as follows;

1.0 IT continuity and DR plans will be developed for all critical business processes to minimise the impact of IT systems failures or disasters.

2.0 IT Continuity and DR planning must be developed in the context of a university wide Business Continuity Management Plan.

3.0 A single framework of IT continuity and DR plans will be maintained to ensure that all levels of planning are consistent.

4.0 IT continuity and DR plans will be tested on an annual basis.

5.0 IT continuity and DR plans will be regularly updated to protect the investment in developing the initial plan and to ensure its continuing effectiveness.

The {system name} IT Continuity Plan also complies with the following regulatory and departmental policies:

{Add any additional regulations or policies to this list}

1.5 RECORD OF CHANGES

Modifications made to this plan since the last printing are as follows;

Record of Changes			
Page No.	**Change Comment**	**Date of Change**	**Signature**

2. OPERATIONAL CONCEPTS

2.1 SYSTEM DESCRIPTION AND ARCHITECTURE

{Provide a general description of the system/s architecture and functionality. Indicate the operating environment, physical location, general location of users and partnerships with external organizations/systems. Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures. Provide a diagram of the architecture, including security controls and telecommunications connections}

2.2 LINE OF SUCCESSION

The {senior authorizing role} is responsible for ensuring the safety of personnel and the execution of procedures documented within this {system name} IT Continuity Plan. If the {senior authorizing role} is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the {delegated authorizing role} shall function as that authority.

{Continue description of succession as applicable}

2.3 RESPONSIBILITIES

The following teams have been developed and trained to respond to an IT Continuity event affecting the {system name}.

The IT Continuity Plan establishes several teams assigned to participate in recovering {system name} operations. The {team name} is responsible for recovery of the {system name} computer environment and all applications. Members of the {team name} include personnel who are also

responsible for the daily operations and maintenance of {system name}. The {team leader title} directs the {team name}.

{Continue to describe each team, their responsibilities, leadership, and coordination with other applicable teams during a recovery operation}

The relationships of the team leaders involved in system recovery and their member teams are illustrated in the diagram below.

{Insert hierarchical diagram of recovery teams. Show team names and leaders; do not include actual names of personnel}

{Describe each team separately, highlighting overall recovery goals and specific responsibilities. Do not detail the procedures that will be used to execute these responsibilities. These procedures will be itemized in the appropriate phase sections below}

3. NOTIFICATION AND ACTIVATION PHASE

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to {system name}. Based on the assessment of the event, the plan may be activated by the {faculty or PAC name} IT Continuity Planning Coordinator.

In an emergency, the {faculty or PAC name}'s top priority is to preserve the health and safety of its staff before proceeding to the Notification and Activation procedures.

Contact information for key personnel is located in the appendices at the end of this document. The notification sequence is listed below:

- The first responder is to notify the {faculty or PAC name} **IT Continuity Planning Coordinator**. All known information must be relayed to the {faculty or PAC name} **IT Continuity Planning Coordinator**.
- The **systems manager** is to contact the **Damage Assessment Team Leader** and inform them of the event. The {faculty or PAC name} **IT Continuity Planning Coordinator** is to instruct the **Damage Assessment Team Leader** to begin assessment procedures.
- The **Damage Assessment Team Leader** is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed locally because of unsafe conditions, the **Damage Assessment Team** is to follow the outline below.

Damage Assessment Procedures

{Detailed procedures should be outlined to include activities to determine the cause of the disruption; potential for additional disruption or damage; affected physical area and status of physical infrastructure; status of IT equipment functionality and inventory, including items that will need to be replaced; and estimated time to repair services to normal operations}

- Upon notification from the {faculty or PAC name} **IT Continuity Planning Coordinator**, the **Damage Assessment Team Leader** is to …

- The **Damage Assessment Team** is to ….

Alternate Assessment Procedures

- Upon notification from the {faculty or PAC name} **IT Continuity Planning Coordinator**, the **Damage Assessment Team Leader** is to …
- The **Damage Assessment Team** is to ….

  - When damage assessment has been completed, the **Damage Assessment Team Leader** is to notify the {faculty or PAC name} **IT Continuity Planning Coordinator** of the results.
  - The {faculty or PAC name} **IT Continuity Planning Coordinator** is to evaluate the results and determine whether the IT Continuity plan is to be activated and if relocation is required.
  - Based on assessment results, the {faculty or PAC name} **IT Continuity Planning Coordinator** is to notify assessment results to civil emergency personnel (e.g. police, fire) as appropriate.

The IT Continuity Plan is to be activated if one or more of the following criteria are met:

1. {System name} will be unavailable for more than 48 hours
2. Facility is damaged and will be unavailable for more than 24 hours
3. {Other criteria, as appropriate}

If the plan is to be activated, the {faculty or PAC name} **IT Continuity Planning Coordinator** is to notify all **Team Leaders** and inform them of the details of the event and if relocation is required.

Upon notification from the {faculty or PAC name} **IT Continuity Planning Coordinator**, **Team Leaders** are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.

The {faculty or PAC name} **IT Continuity Planning Coordinator** is to notify the off-site storage facility that an IT Continuity event has been declared and to ship the necessary materials (as determined by damage assessment) to the alternate site.

The {faculty or PAC name} **IT Continuity Planning Coordinator** is to notify the alternate site that an IT Continuity event has been declared and to prepare the facility for the {faculty or PAC name}'s arrival.

The {faculty or PAC name} **IT Continuity Planning Coordinator** is to notify remaining personnel (via notification procedures) on the general status of the incident.

4. RECOVERY OPERATIONS

This section provides procedures for recovering the application at the alternate site, whereas other efforts are directed to repair damage to the original system and capabilities.

The following procedures are for recovering the {system name} at the alternate site. Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

{**Recovery Goal.** State the **first** recovery objective as determined by the business risk assessment. For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.

{team name}

Team Recovery Procedures

{team name}

Team Recovery Procedures

{team name}

Team Recovery Procedures

Recovery Goal. State the **second** recovery objective. For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.

{team name}

Team Recovery Procedures

{team name}

Team Recovery Procedures

{team name}

Team Recovery Procedures

Recovery Goal. State the **remaining** recovery objectives. For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures}

5. RETURN TO NORMAL OPERATIONS

This section discusses activities necessary for restoring {system name} operations at the {faculty or PAC name}'s original or new site. When the computer facility at the original or new site has been restored, {system name} operations at the alternate site must be transitioned back. The goal is to provide a seamless transition of operations from the alternate site to the original or new computer facility.

Original or New Site Restoration

{Procedures should be outlined, per necessary team, to restore or replace the original site so that normal operations may be transferred. IT equipment and telecommunications connections should be tested}

{team name}

Team Restoration Procedures

{team name}

Team Restoration Procedures

{team name}

Team Restoration Procedures

5.1 CONCURRENT PROCESSING

{Procedures should be outlined, per necessary team, to operate the system in coordination with the system at the original or new site. These procedures should include testing the original or new system until it is functioning properly and the IT Continuity system is shut down gracefully}

{team name}

Team Restoration Procedures

{team name}

Team Restoration Procedures

5.2 PLAN DEACTIVATION

(Procedures should be outlined, per necessary team, to clean the alternate site of any equipment or other materials belonging to the {faculty or PAC name}, with a focus on handling sensitive information. Materials, equipment, and backup media should be properly packaged, labeled, and shipped to the appropriate location(s).Team members should be instructed to return to the original or new site}

{team name}

Team Testing Procedures

{team name}

Team Testing Procedures

6. PLAN APPENDICES

{The appendices included should be based on system and plan requirements}

- Personnel Contact List
- Vendor Contact List
- Equipment and Specifications
- Service Level Agreements and Memorandums of Understanding
- IT Standard Operating Procedures
- Business Risk Assessment
- Related IT Continuity Plans
- Emergency Management Plan
- Emergency Evacuation Plan