



DISASTER RECOVERY PLAN



Company: Town of Caledon

Date: insert date

Version: DRAFT

Document Control

Version History

Version	Date	Comments

Document Owners

Name	Title	Ownership

Introduction

For the purpose of this plan a disaster is defined as any event whose impact would fit the following criteria:

SYSTEMS	<i>Core operational systems which allow IT to deliver services are not available for over 4 hours during working hours</i>
SERVICES	<i>No Connectivity available for over 4 hours</i>
SITE	<i>Unable to access site for any period more than 4 business hours</i>

Detailed Response Strategy

SYSTEMS	Core operational systems which allow IT to deliver services are not available for over 4 hours during working hours	
Hardware Component Failure		
Planned Response Strategy	Expected Response Results	Post-Disaster Expectations
<i>Assess situation then enable Disaster Recovery Plan if required for systems affected.</i> <i>Contact Hardware vendor, identify if replacement can be procured before SLA's have been infringed.</i> <i>Restore systems on site if possible – allow 24-hour time frame before DRP is enacted in full</i>	<i>100% of core infrastructure will be available on site or at the DR site</i> <i>100% of Critical applications and services will be available within 5 days on site or at the DR site. Important and minor systems to be functionally restored within 3 days</i>	<i>Disaster Recovery site will be restored to production systems.</i> <i>Build more hardware redundancy if required</i>

Sample Failures:

Software, Software Compatibility, Coding Errors or Bugs, Security Breaches, Virus, Data Loss, Human Error

Information Technology Statement of Intent

This document delineates Town policies and procedures for technology disaster recovery, as well as our process-level plans for recovering critical technology platforms and the telecommunications infrastructure. This document summarizes our recommended procedures. In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of our people, our systems, and our data.

Our mission is to ensure information system uptime, data integrity and availability, and business continuity for the Town of Caledon.

Policy Statement

Corporate management has approved the following policy statement:

- The Town shall develop a comprehensive IT disaster recovery plan;
- A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan;
- The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities;
- The disaster recovery plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed;
- All staff must be made aware of the disaster recovery plan and their own respective roles; and
- The disaster recovery plan is to be kept up to date to take into account changing circumstances.

Objectives

The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the Town recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

1. The need to ensure that all employees fully understand their duties in implementing such a plan;
2. The need to ensure that operational policies are adhered to within all planned activities;
3. The need to ensure that proposed contingency arrangements are cost-effective;
4. The need to consider implications on other corporate sites; and
5. Disaster recovery capabilities as applicable to key customers, vendors and others.

Staffing Requirements

Initial Assessment Team

It is the responsibility of the Initial Assessment Team to assess the level of impact and deploy the Disaster Recovery Plan (DRP) as they see appropriate. The IAT has the authority to invoke the plan if the impact is predicted to be as above rather than waiting for it to be a known.

The assessment team consists of the following individuals:

Primary		
Name	Mobile	Email
Erin Britnell Interim Manager, Information Technology	416-550-1437	Erin.Britnell@caledon.ca
Secondary		
Name	Mobile	Email
Nicholas Alleyne Supervisor, IT Operations and Infrastructure	416-428-7778	Nicholas.Alleyne@caledon.ca
Melissa Yardy Supervisor, IT Corporate Solutions	416-819-2339	Melissa.Yardy@caledon.ca

***Note:** In absence of the primary assessment team member(s) a secondary team member will have the authority to declare a disaster and invoke the DRP.*

Incident Management Team

Comprises management, technical and other support staff who will be responsible for notification of all relevant staff, activation of recovery services provided by third party organizations and establishing operational capability at the Town Administration building. The team is also responsible for the overall management of recovery activities.

Operations Team

Designated operational staff will relocate to **(DR site or engage DR vendor etc.)** once the Incident Management Team has agreed a schedule for relocation and operational capability at the Recovery Centre has been established.

Other Staff

Staff not designated for immediate relocation to another site will, where possible, undertake such work activities from home as are possible and agreed with their department manager. Where this is not possible, staff will await instructions and remain at home until such time as the Town Administration building becomes available or alternate accommodation can be provided.

Notification Calling Tree

Call Tree (to be structured):

Discoverer calls their supervisor: Nicholas or Melissa. If neither are available calls Erin. Management team (Nicholas, Melissa, Erin) contact remaining members of IT team. Communication role handled members of the management team.

Key Personnel Contact Information (Internal)

Disaster Recovery Team		
Name, Title	Contact Option	Contact Information
Ankur Arora Administrator, Server and Network	Mobile	416-805-3256
	Email	Ankur.Arora@caledon.ca
	Alternate Email	
Nicholas Alleyne Supervisor, IT Operations and Infrastructure	Mobile	416-428-7778
	Email	Nicholas.Alleyne@caledon.ca
	Alternate Email	
Krunal Barot Administrator, Server and Network	Mobile	647-444-5070
	Email	Krunal.Barot@caledon.ca
	Alternate Email	
Adam Weiler Administrator, End User Computing	Mobile	416-358-1526
	Email	Adam.Weiler@caledon.ca
	Alternate Email	
Abhijit Boro Administrator, Database and Application	Mobile	416-659-7467
	Email	Abhijit.Boro@caledon.ca
	Alternate Email	
Aruna Liyanage Administrator, Database and Application	Mobile	416-578-8003
	Email	Aruna.Liyanage@caledon.ca
	Alternate Email	
Abbey Akinrinola Developer, Web Applications	Mobile	647-376-4857
	Email	Abbey.Akinrinola@caledon.ca
	Alternate Email	
Lori Allard Technician, Help Desk	Mobile	647-273-3869
	Email	Lori.Allard@caledon.ca
	Alternate Email	
Ruchira Welikala Coordinator, GIS	Mobile	647-519-5802
	Email	Ruchira.Welikala@caledon.ca
	Alternate Email	
Melissa Yardy Supervisor, IT Corporate Solutions	Mobile	416-819-2339
	Email	Melissa.Yardy@caledon.ca
	Alternate Email	
Erin Britnell Interim Manager, Information Technology	Mobile	416-550-1437
	Email	Erin.Britnell@caledon.ca
	Alternate Email	

Key Personnel Contact Information (External)

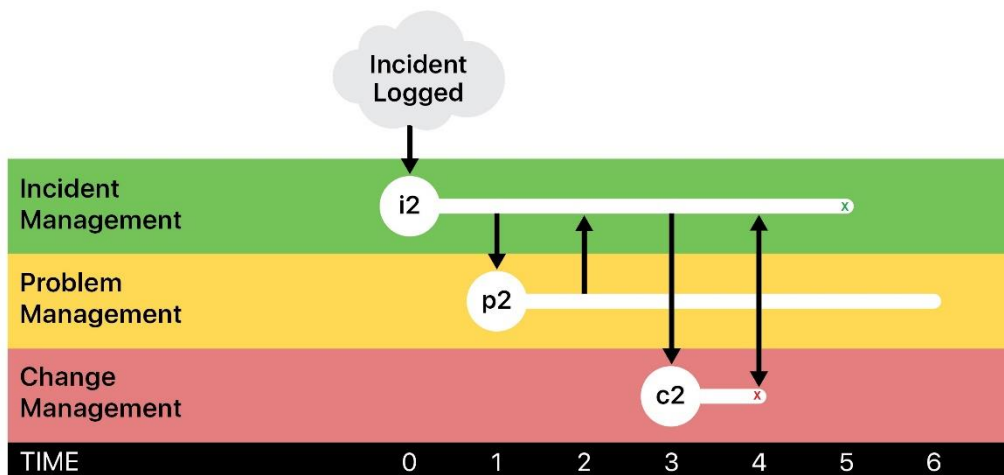
Name, Title	Contact Option	Contact Information
	<i>Work</i>	
	<i>Mobile</i>	
	<i>Email</i>	
	<i>Work</i>	
	<i>Mobile</i>	
	<i>Email</i>	
	<i>Work</i>	
	<i>Mobile</i>	
	<i>Email</i>	
	<i>Work</i>	
	<i>Mobile</i>	
	<i>Email</i>	
	<i>Work</i>	
	<i>Mobile</i>	
	<i>Email</i>	
	<i>Work</i>	
	<i>Mobile</i>	
	<i>Email</i>	
	<i>Work</i>	
	<i>Mobile</i>	
	<i>Email</i>	

IT Service Continuity Management

Incident Management Process Flow

INCIDENT MANAGEMENT - PROBLEM MANAGEMENT - CHANGE MANAGEMENT

PROCESS FLOW



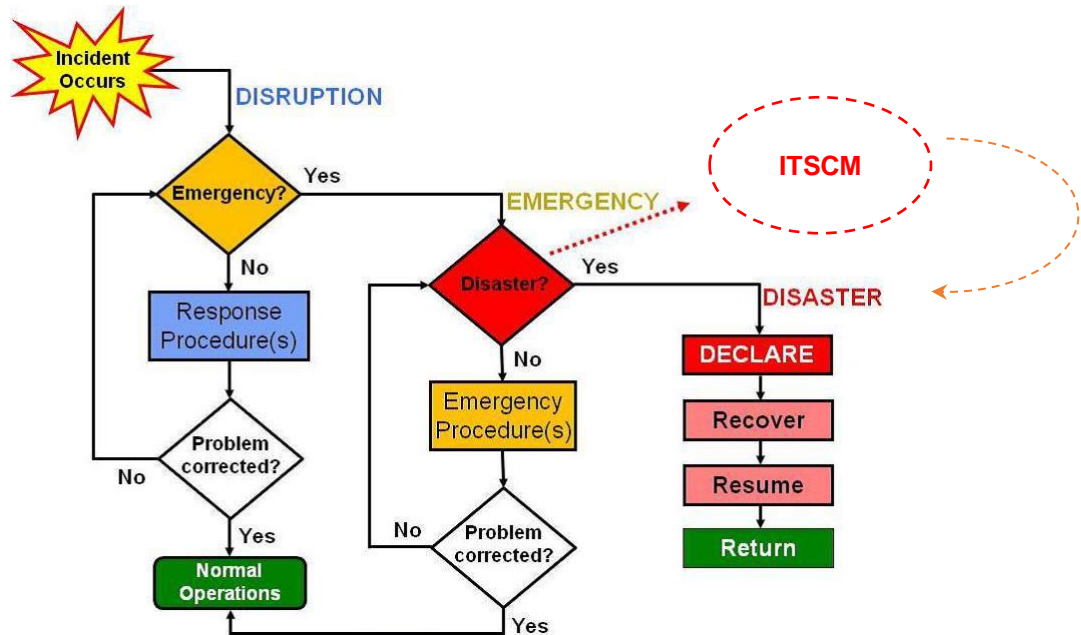
- At **TIME = 0**, an External Event is detected by the Incident Management process. This could be as simple as a user calling to say that a service is unavailable or it could be an automated alert from a system monitoring device.

The incident is logged and classified as incident **i2**. Then, the incident owner tries to match **i2** to known errors, work-arounds, or temporary fixes, but cannot find a match in the database.

- At **TIME = 1**, the incident owner creates a problem request to the Problem Management process anticipating a work-around, temporary fix, or other assistance. In doing so, the incident owner has prompted the creation of Problem **p2**.
- At **TIME = 2**, the problem owner of **p2** returns the expected temporary fix to the incident owner of **i2**. Note that both **i2** and **p2** are active and exist simultaneously. The incident owner for **i2** applies the temporary fix.
- In this case, the work-around requires a change request. So, at **Time = 3**, the incident owner for **i2** initiates change request, **c2**.
- The change request **c2** is applied successfully, and at **TIME = 4**, **c2** is closed. Note that for a while **i2**, **p2** and **c2** all exist simultaneously.
- Because **c2** was successful, the incident owner for **i2** can now confirm that the incident is resolved. At **TIME = 5**, **i2** is closed. However, **p2** remains active while the problem owner searches for a permanent fix. The problem owner for **p2** would be responsible for implementing the permanent fix and initiating any necessary change requests.

IT Service Continuity Management

ITSCM goes far beyond other ITIL processes such as Incident Management. For example, the second one focuses on dealing with less significant events; while Service Continuity Management is more related to those incidents than to their impact on the organization; they can be classified as disastrous. This classification may vary from company to company, but it always includes those events whose incidence is capable of interrupting Business Continuity.



Recovery Procedures

Data and Backups

Current DR Recovery Capabilities

Disaster Recovery Activation Procedures

The following list sets out the main tasks to be undertaken in plan activation. It is possible however that the Incident Management Team will be required to modify these tasks and or sequence in order to meet the circumstances pertaining at the time of the event.

	Activities
1	Contact DR Team and advise of formal invocation.
2	Activate IT Services Technical Recovery Plans (as required)
3	Contact any external IT service providers, inform them of the situation and request activation of their procedures to switch delivery of services to the alternative premises (if required).
4	Contact Data Communications services provider; inform them of the situation and request activation of their procedures to switch data communications to the alternative premises as required.
5	Contact telephony provider and request activation of their procedures to switch numbers to the alternative premises.
6	Inform staff of actions taken and what is required of them in the short and longer term. Confirm which staff will relocate to the alternative premises.
7	Agree staff transportation arrangements for staff transferring to DR site
8	Notify insurance company via broker for future claim (as required)
9	Review key contact list and complete any outstanding contacts.
10	Initiate formal status reporting system to cover: <ul style="list-style-type: none"> Recovery activities – tasks undertaken, responsibilities and completion timetable. Recovery costs tracking – set up cost centre and reporting mechanism.

Failback Procedures

Current System Architecture

IT Systems

This section will be high-level and refer to DR Playbook

Plan Maintenance and Testing

While efforts will be made initially to construct this DRP in as complete and accurate a manner as possible, it is essentially impossible to address all possible problems at any one time. Additionally, over time the Disaster Recovery needs of the enterprise will change. As a result of these two factors this plan will need to be tested on a periodic basis to discover errors and omissions and will need to be maintained to address them.

Maintenance

The DRP will be updated annually or any time a major system update or upgrade is performed, whichever is more often. The Disaster Recovery Lead will be responsible for updating the entire document, and so is permitted to request information and updates from other employees and departments within the organization in order to complete this task.

Maintenance of the plan will include (but is not limited to) the following:

- Ensuring that call trees are up to date
- Ensuring that all team lists are up to date
- Reviewing the plan to ensure that all of the instructions are still relevant to the organization
- Making any major changes and revisions in the plan to reflect organizational shifts, changes and goals
- Ensuring that the plan meets any requirements specified in new laws
- Other organizational specific maintenance goals

During the Maintenance periods, any changes to the Disaster Recovery Teams must be accounted for. If any member of a Disaster Recovery Team no longer works with the company, it is the responsibility of the Disaster Recovery Lead to appoint a new team member.

Testing

The Town of Caledon is committed to ensuring that this DRP is functional. The DRP should be tested annually in order to ensure that it is still effective. Testing the plan will be carried out as follows:

1. Walkthroughs - Team members verbally go through the specific steps as documented in the plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses. This test provides the opportunity to review a plan with a larger subset of people, allowing the DRP project manager to draw upon a correspondingly increased pool of knowledge and experiences. Staff should be familiar with procedures, equipment, and offsite facilities (if required).
2. Simulations - A disaster is simulated so normal operations will not be interrupted. Hardware, software, personnel, communications, procedures, supplies and forms, documentation, transportation, utilities, and alternate site processing should be thoroughly tested in a simulation test. However, validated checklists can provide a reasonable level of assurance for many of these scenarios. Analyze the output of the previous tests carefully before the proposed simulation to ensure the lessons learned during the previous phases of the cycle have been applied.

3. Parallel Testing - A parallel test can be performed in conjunction with the checklist test or simulation test. Under this scenario, historical transactions, such as the prior business day's transactions are processed against preceding day's backup files at the contingency processing site or hot site. All reports produced at the alternate site for the current business date should agree with those reports produced at the alternate processing site.
4. Full-Interruption Testing - A full-interruption test activates the total DRP. The test is likely to be costly and could disrupt normal operations, and therefore should be approached with caution. The importance of due diligence with respect to previous DRP phases cannot be overstated.
5. Any gaps in the DRP that are discovered during the testing phase will be addressed by the Disaster Recovery Lead as well as any resources that he/she will require.

