DISASTER RECOVERY PLAN

Company: Grey County
Date: August 24th , 2019
Version: DRAFTv3

Document Control

Version History

Version	Date	Comments
vDRAFT	May 2nd, 2019	To be reviewed
vDRAFT	July 24th, 2019	To be reviewed
vDRAFT	August 24th, 2019	Added contacts – p8/9

Document Owners

Name	Title	Ownership

Glossary of Terms, Abbreviations, and Acronyms

DRP	DISASTER RECOVERY PLAN - The management approved document that defines the resources, actions, tasks and data required to manage the technology recovery effort. Usually refers to the technology recovery effort.
DR SITE	DISASTER RECOVERY SITE - An alternate site used to re-establish information technology services (including components such as infrastructure, telecommunications, systems, applications and data) following a disruption of IT services.
ITIL	Formerly an acronym for Information Technology Infrastructure Library, is a set of detailed practices for IT service management that focuses on aligning IT services with the needs of business.
ITSCM	INFORMATION TECHNOLOGY SERVICE CONTINUITY MANAGEMENT – A discipline used to ensure continuity of IT service in time of any disaster.
RPO	RECOVERY POINT OBJECTIVE - The point in time to which data is restored and/or systems are recovered after an outage.
RTO	RECOVERY TIME OBJECTIVE - The period of time within which systems, applications, or functions must be recovered after an outage.
SLA	SERVICE LEVEL AGREEMENT - A formal agreement between a service provider (whether internal or external) and their client (whether internal or external), which covers the nature, quality, availability, scope and response of the service provider.

Introduction

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

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

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
Assess situation then enable Disaster Recovery Plan if required for systems affected. *Contact Hardware vendor, identify if replacement can be procured before SLA's have been infringed.* *Restore systems on site if possible – allow 24-hour time frame before DRP is enacted in full*	*100% of core infrastructure will available on site or at the DR site* *100% of Critical applications and services will be available within 4 hours on site or at the DR site.* *Important and minor systems to be functionally restored within 3 days*	*Disaster Recovery site will be restored to production systems.* *Build more hardware redundancy if required*

Software Failure

Planned Response Strategy	Expected Response Results	Post-Disaster Expectations
Assess situation then enable Disaster Recovery Plan if required for systems affected. *Contact software vendor or in-house developer for support, upgrades, revisions or patches.* *Restore last known working version of the software stack.* *Restore systems on site if possible – 4 hour SLA before DRP enacted in full*	*100% of core infrastructure will available on site or at the DR site* *100% of Critical applications and services will be available within 4 hours on site or at the DR site.* *Important and minor systems to be restored within 3 days*	*Ensure that strict quality controls are placed on the operational environments.* *Develop roll back procedures.*

Security Breaches

Planned Response Strategy	Expected Response Results	Post-Disaster Expectations
Assess situation then enable Disaster Recovery Plan if required for systems affected. *Identify the systems affected. Take appropriate action, permissions, take off line. Eliminate security breach.* *Restore systems on site if possible.*	***Security breach must be closed before activating redundant DR systems.*** *100% of core infrastructure will available on site or at the DR site.* *100% of Critical of applications and services will be available within 4 hours on site or at the DR site.*	*Assess security breach, identify audits, patches or any mitigation routines that could prevent this event.* *Take legal or disciplinary action if required.* *If physical breach, review security procedures with facilities and mitigate.*

Virus

Planned Response Strategy	Expected Response Results	Post-Disaster Expectations
Assess situation then enable Disaster Recovery Plan if required for systems affected. *Identify the systems affected. Take appropriate action, update virus definition, patch and deploy if required.* *Restore systems on site if possible. Use systems restore procedures.*	***Virus incident must be eliminated or isolated before activating redundant DR systems.*** *100% of core infrastructure will available on site or at the DR site.* *100% of Critical applications and services will be available within 4 hours on site or at the DR site.*	*Assess virus incident identify audits, patches or any mitigation routines that could prevent this event.* *Take legal or disciplinary action if required.*

Data Loss

Planned Response Strategy	Expected Response Results	Post-Disaster Expectations
Assess situation then enable Disaster Recovery Plan if required for systems affected. *Restore data from archives. Use systems restore procedures.*	*100% of core infrastructure will be available on site or at the DR site.* *100% of Critical applications and services will be available within 4 hours on site or at the DR site.*	*Enable strict controls around data, audit systems and ensure correct permissions are set per data set.*

Human Error

Planned Response Strategy	Expected Response Results	Post-Disaster Expectations
Assess situation then enable Disaster Recovery Plan if required for systems affected. *Restore systems from backups. Use systems restore procedures.*	*Eliminate error; ensure there is no replication to DR systems.* *100% of core infrastructure will be available on site or at the DR site.* *100% of Critical of applications and services will be available within 4 hours on site or at the DR site.*	*Training, documentation, limit access to systems.*

SERVICES	***No Connectivity available for over 4 hours***

Power Failure

Planned Response Strategy	Expected Response Results	Post-Disaster Expectations
Establish if wider electricity cut or issue with premises. *If local area outage, seek timelines for rectification and act accordingly* *If within building, facilities to act immediately to rectify*	*Full power to be restored within 4 hours* *If catastrophic invoke DRP*	*If internal issue seek program of maintenance to avoid future incidents.*

Telephony Failure

Planned Response Strategy	Expected Response Results	Post-Disaster Expectations
Assess situation then enable Disaster Recovery Plan if required for systems affected. *Contact provider for immediate engineer investigation – 2 hour SLA expected for resolution* *Move staff if appropriate.* *Restore systems on site if possible.*	*100% of core infrastructure will be available on site or at the DR site* *100% of Critical of applications and services will be available within 4 hours on site*	*Once the Network is again accessible, restore to production systems.*

SITE	***Unable to access site for any period more than 4 business hours***

Administration Building Cannot be Accessed

Planned Response Strategy	Expected Response Results	Post-Disaster Expectations
Assess situation then enable Disaster Recovery Plan if required for systems affected. *The cause will determine likely time and cost of impact* *-Fire* *-Structural Failure* *-Power Failure* *-Water Damage* *-Vandalism* *-Unique Circumstances* *Move staff as and if appropriate.*	*100% of all core infrastructure will be available immediately at DR Site* *100% of Critical applications and services will be available within 4 hours at DR site. Important and minor systems to be restored.*	*Once the office is again accessible, restore to production systems.*

Information Technology Statement of Intent

This document delineates our 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

Policy Statement

Corporate management has approved the following policy statement:

- The County 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 (including LTC).
- 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.
- 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 County 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 (DR Team)

Initial Assessment Team

It is the responsibility of the Initial Assessment Team (IAT) 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. *(should have at least one individual who is part of a corporate wide Crisis Management Team)*

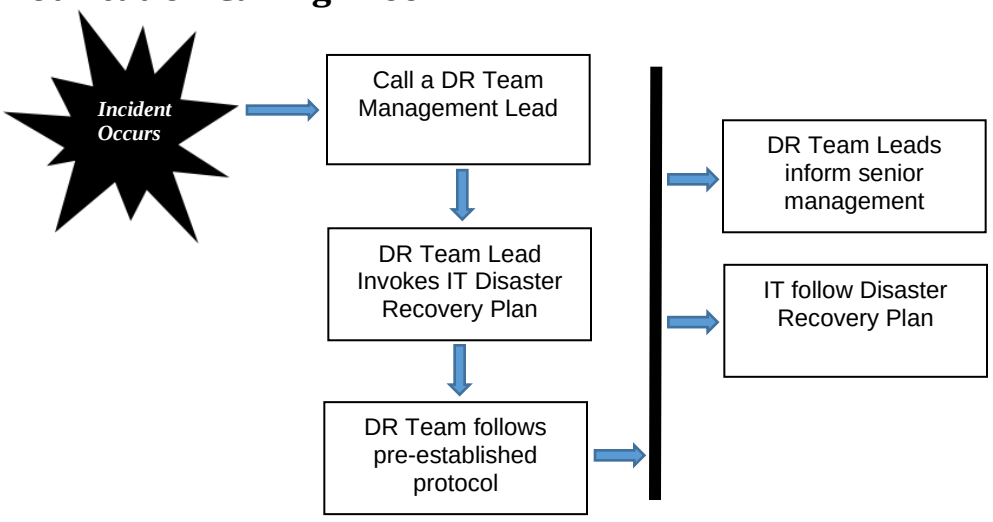
The assessment team consists of the following individuals:

Primary		
Name	**Mobile**	**Email**
Jody MacEachern Senior Manager, Information Technology	519-378-4493	Jody.MacEachern@Grey.ca
Kevin Weppler, Director of Finance	519-375-0504	Kevin.Weppler@Grey.ca
Secondary		
Name	**Mobile**	**Email**
Evan Davis Technology & Infrastructure Manager	519-378-4992	Evan.Davis@Grey.ca
Neil Ecker Senior Programmer	519-377-2198	Neil.Ecker@Grey.ca

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 County Administration building. The team is also responsible for the overall management of recovery activities.

Notification Calling Tree



Key Personnel Contact Information (Internal)

Name, Title	Contact Option	Contact Information
IT Support Team		
Brian Richards Information Services Coordinator	***Mobile***	(519) 372-0219 x 1524
	Email	brian.richards@grey.ca
	Alternate Email	
Keith Hillman Information Services Coordinator	***Mobile***	(519) 372-0219 x 1534
	Email	keith.hillman@grey.ca
	Alternate Email	
Alex Amundson Information Services Coordinator	***Mobile***	(519) 372-0219 x 1525
	Email	alex.amundson@grey.ca
	Alternate Email	
Kevin Woods Helpdesk Analyst	***Mobile***	
	Email	kevin.woods@grey.ca
	Alternate Email	
Brad Fritz, Business Analyst Programmer	***Mobile***	
	Email	brad.fritz@grey.ca
	Alternate Email	
Matt Taylor, Systems Analyst	***Mobile***	226-668-6973
	Email	matt.taylor@grey.ca
	Alternate Email	
Kim Wingrove, CAO	***Mobile***	519-372-0219
	Email	kim.wingrove@grey.ca
	Alternate Email	
Marlene McLevy, Emergency Systems Coordinator / Claims Supervisor	***Mobile***	519-378-3101
	Email	marlene.mclevy@grey.ca
	Alternate Email	
Robert Hatten, Communications Manager	***Mobile***	519-373-1592
	Email	robert.hatten@grey.ca
	Alternate Email	
Departmental Contacts		
Kevin McNab, Director of Paramedic Services		519-379-0279
		kevin.mcnab@grey.ca
Pat Hoy, Director of Transportation		519-379-0703
		pat.hoy@grey.ca
VACANT Director of Long Term Care,		
Barb Fedy, Director of Social Services		519-378-4767
		barb.fedy@grey.ca
Anne Marie Shaw, Director of Housing		519-374-4900
		annemarie.shaw@grey.ca

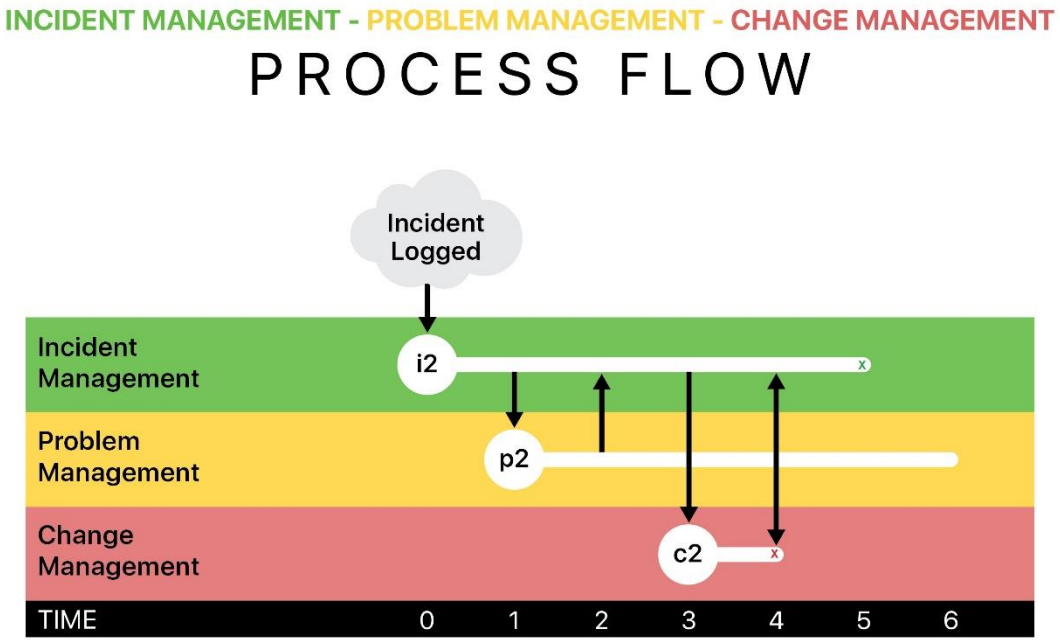
Key Personnel Contact Information (External)

Name	Role	Phone	Email	Notes
Teresa Maslach	Senior Policy and Business Advisor	M: 647-961-9859T: (416) 326-5623	Teresa.Maslach@ontario.ca	ICON / Courts
Owen Sound Police Dispatch	Road Closure Information			

IT Service Continuity Management

Incident Management Process Flow

Below is the ITIL recommended process flow for incident management:



- *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.

Refer to *Figure 1* for a detailed overview of the County's recommended process flow at time of disaster (TOD).

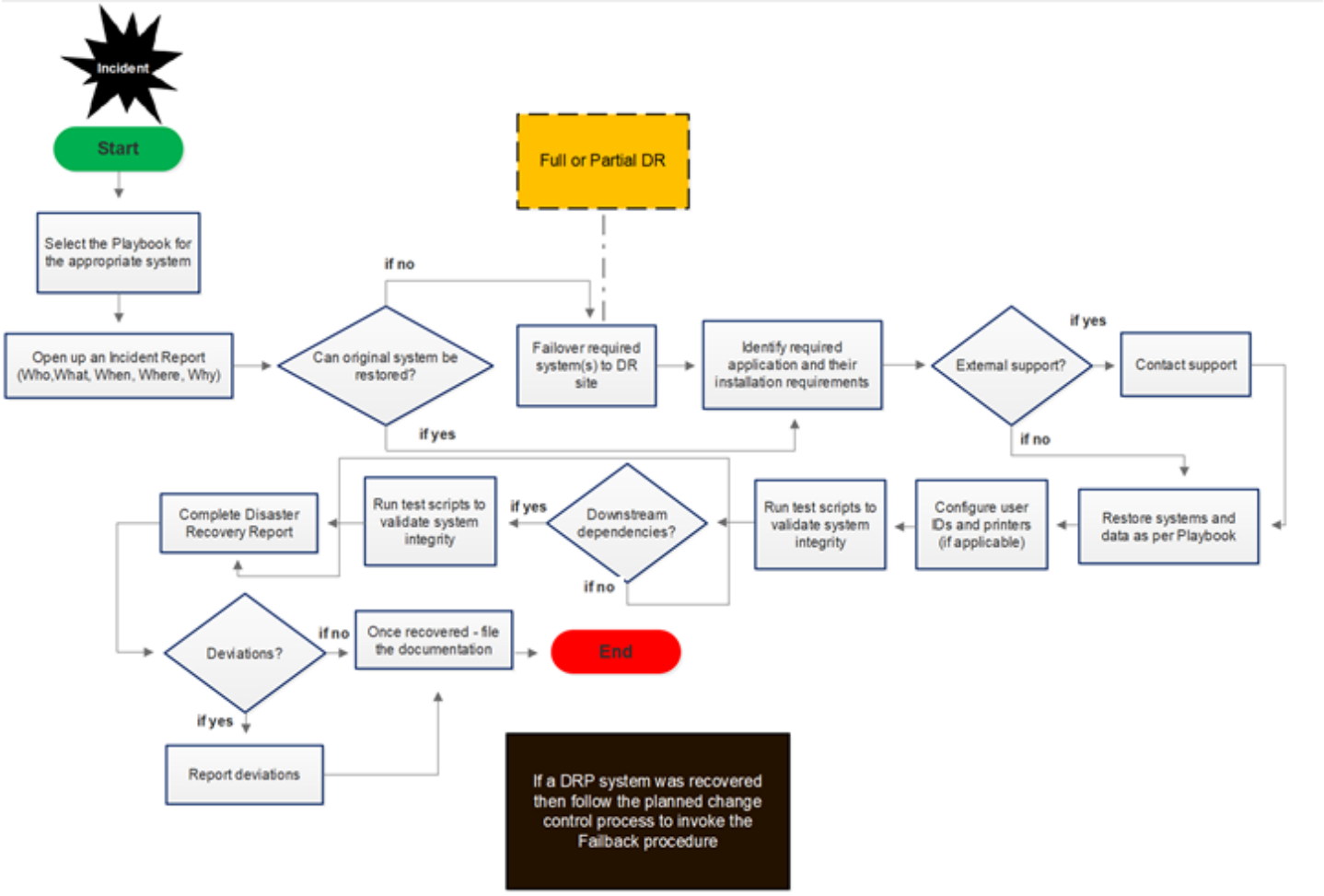


Figure 1- Grey County DR Process Flow (Recommended)

Recovery Procedures

Data and Backups

Corporate Environment (VxRail at Administration Building)
Virtual machines are stored in one of the following VM folders within vCenter, which determines the retention and backup schedule.
Tier 1 Machines
• Daily incrementals starting at 2100h with a weekly full created on Saturdays to the EMC storage appliance at the Administration Building • 14 daily restore points are kept onsite at the administration building • Backups are transferred to Grey Gables over the WAN, keeping 4 daily 3 weekly and 6 monthly backups • A backup copy job at Administration Building keeps 4 weekly and 12 monthly backups onsite
Tier 2 Machines
• Daily incrementals starting after Tier 1 finishes with a weekly full created on Saturdays to the EMC storage appliance at the Administration Building • 30 restore points are kept onsite at the administration building • Backups are transferred to Grey Gables over the WAN, keeping 4 daily 3 weekly and 4 monthly backups
Tier 3 Machines
• Daily incrementals starting after Tier 2 finishes with a weekly full created on Saturdays to the EMC storage appliance at the Administration Building • 14 restore points are kept onsite at the administration building • Backups are transferred to Grey Gables over the WAN, keeping 3 daily and 2 weekly backups • Tier 4 Machines (Non-production workloads such as development environments • These VMs are not backed up at all. • Beachell (main SQL server) is in this folder and is backed up using SQL agent jobs. The files are copied using SyncBack to the EMC storage appliance at the administration building. We require additional storage at the offsite location to replicate these files. There was an issue with using Veeam to back this machine up in the past, which prompted this alternate backup strategy • Veeam (Contains the main Veeam server, and the Veeam proxies) • These VMs are not backed up at all. • VMware HCIA Folder (Contains the VMs critical to the functioning of VxRail itself) • Daily incrementals at 1800h with a weekly full created on Saturdays to the EMC storage appliance at the Administration Building • 14 restore points are kept at Admin building • This job is not replicated offsite. In a total site disaster, the cluster would need to be rebuilt, and having backups of these VMs would not serve any useful purpose in that case.

Long-Term Care Facilities
Each LTC home has its own Veeam server to perform local backups, and they trade backups with each other daily for offsite backups.
Grey Gables
• Daily incrementals at 20:00h with weekly full created on Saturdays to the local QNAP • 14 restore points are kept locally • Previous 3 days backups copied to Lee Manor
Lee Manor
• Daily incrementals at 2000h with weekly full created on Saturdays to the local QNAP • 14 restore points are kept locally • Previous 3 days backups copied to Grey Gables
Rockwood Terrace
• Daily incrementals at 2000h with weekly full created on Saturdays to the local QNAP • 14 restore points are kept locally • Previous 3 days backups copied to Grey Gables

Current DR Recovery Capabilities

There are currently no formal disaster recovery procedures in place at the County. If there was a site disaster today, the County would attempt to order new equipment (as required) from third-party supplier CDW.

A current Recovery Time Actual (RTA) has not been formally tested at this point in time. The recovery process could result in an outage of >7-days based on equipment delivery and recovery activity estimates.

This has been identified as a key vulnerability in BIA report.

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 (refer to Playbooks 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 (as required).
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 (as required).
7	Arrange for staff transferring to alternate site(s) (if applicable)
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: • Recovery activities – tasks undertaken, responsibilities and completion timetable. • Recovery costs tracking – set up cost centre and reporting mechanism.

Service Order of Recovery

Order of Restoration Table – Core Infrastructure & IT Business Systems (Tier 1 and Tier 2)

Primary Data Centre - Administration Building - 595 9th Ave East

This table details the order recovery for core business applications (Tier1&2) and supporting IT technology *i.e. which infrastructure components to restore and in which order (see Figure 2 for Application/Database mapping).*

It should take into account application dependencies, authentication, middleware, database and third-party elements and list restoration items by system or service type. Ensure this order of restoration in understood before engaging in recovery activities. The County will build associated "Playbooks" for each of the items detailing the technical steps for recovery. These Playbooks can be added to this document as Annexures or developed as standalone documents.

#	Activity/Device (*business system)	System/Service Description	Notes
1	Assemble Recovery Team	Ensure that the required recovery team members have been contacted	*Refer to "Contact Information" in Section 1 of this document*
	Core Infrastructure		
2	UPS	Power On	Wait to see if unit powers on after checks
2.1	UPS	Backup	If a UPS does not come online remove the twist lock cable for the PDU(s) from the down UPS and move to the other UPS
3	PDU	Physically look for power indicator lights	Once UPSs come online these units should make a clicking sound (a lot of them)
3.1	PDU	Backup	If it is one of the vertical PDUs this is fine all of those units have backup power supplies or redundant equipment
3.2	PDU	Backup	If a UPS is down and a horizontal unit has no power try moving the step down unit to the next UPS
3.3	PDU	Backup	If the Stepdown unit is not functioning unplug the PDU from it and power via wall outlet on west wall (will need extension cord)
4	Top of Rack Switches	Power on	Wait for self check to complete before moving to next step
4.1	Top of Rack Switches	Backup	Redundant units. If neither powers on contact Dell warrany to ASAP ship replacement units. 1-866-362-5350
4.2	Top of Rack Switches	Backup	Replace switch. Config Backups stored here.
5	FortiGates	Power on	If they turn on wait a few minutes for connectivity to come up on its own.
6	VxRail Nodes	Power up all 5 at the same time	Check vSAN health if okay move on if not call EMC Support 1 800 543 4782
6.1	VxRail Nodes	Backup	If not operable will have to move to DR hosting
7	Guest VMs	Power on all VMs	are they on? Is everything up in Nagios? https://alert.grey.ca/nagios
8	MCKNIGHT & WERRY	Start Services (Alfresco entry in LastPass)	Visit https://docs.grey.ca/share
9	GC-SDLC	Power On	Check boot process from KVM
9.1	GC-SDLC	Log In	Check that the connection status to the province.
10	Mitel Voice Switches	Power on	Wait for lights to start blinking

11	End User Switches	Power on	Wait for self check to complete then see if device such as Desk phones and Access Points come online
11.1	End User Switches	Check connectivity	Do you get a DHCP address? Do desk phones work? WiFi working?
11.2	End User Switches	Backup	If we switch dies send away for warranty. We have zero spare units for the stacks in Admin so that stack member will not exist until we replace it.
12	FortiGates	Backup	Grab a spare 2930 48 POE+ and configure it based off of the Switch config backups found here. Depending on what member is missing make sure to copy the config and remove the member number from the port before uploading the config. Remove all ports that are not there in the config before putting in place. (do not overwrite the version in SharePoint)
13	Backup Storage (Dell NX3230 10.10.33.29)	Checking connectivity	Check FortiManager for connectivity and VPN statuses
13.1	Backup Storage (Dell NX3230 10.10.33.29)	Power On	Once powered on all storage should show in Kuhl VM.

Order of Restoration Table – Long-Term Care Facilities

Grey Gables, Lee Manor, Rockwood Terrace

This table details the order recovery for core systems located within the three LTC facilities

#	Activity/Device	System/Service Description	Notes
1	UPS	Power On	Wait to see if unit powers on after checks
1.1	UPS	Backup	If a UPS does not come online remove the twist lock cable for the PDU(s) from the down UPS and move to the other UPS
2	PDU	Physically look for power indicator lights	Once UPSs come online these units should make a clicking sound (a lot of them)
2.1	PDU	Backup	If it is one of the vertical PDUs this is fine all of those units have backup power supplies or redundant equipment
2.2	PDU	Backup	If a UPS is down and a horizontal unit has no power try moving the step down unit to the next UPS
2.3	FortiGates	Power on	If they turn on wait a few minutes for connectivity to come up on its own.
3	Shared Storage	Power on qnaps	Wait for the loud beep several minutes later
4	Host Server	power on	Make sure console boots to ESXi ready screen. If not call Dell Support
5	Host Server	Backup	If not operable will have to move to DR hosting
5.1	Guest VMs	Power on all VMs	are they on? Is everything up in Nagios? https://alert.grey.ca/nagios
6	Guest VMs	Nurse call (Austco paging)	Check if paging is working.
6.1	Mitel Voice Switches	Power on	Wait for lights to start blinking
7	End User Switches	Power on	Wait for self check to complete then see if device such as Desk phones and Access Points come online
8	End User Switches	Check connectivity	Do you get a DHCP address? Do desk phones work? WiFi working?

9	End User Switches	Backup	If we switch dies send away for warranty. We have zero spare units for the stacks in Admin so that stack member will not exist until we replace it.
9.1	End User Switches	Backup	Grab a spare 2930 48 POE+ and configure it based off of the Switch config backups found here. Depending on what member is missing make sure to copy the config and remove the member number from the port before uploading the config. Remove all ports that are not there in the config before putting in place. (do not overwrite the version in SharePoint)
9.2	FortiGates	Checking connectivity	Check FortiManager for connectivity and VPN statuses
10	FortiGates	Power on	If they turn on wait a few minutes for connectivity to come up on its own.

Business Systems			
	Database Services (PostgreSQL)	McDonald (VM)	Upstream dependency – Alfresco, Emergency Contacts and Emergency Management Portal
	Database Services (MariaDB)	Lantz (VM)	Upstream dependency – Corporate Website
	Email	Insert server name	Microsoft Exchange 2010
	ECM (Alfresco)	Insert server name	
	Application Services (Emergency Contacts)	Insert server name	
	Application Services (Emergency Management Portal)	Insert server name	
	Application Services (Corporate Website)	Insert server name	
	Database Services (MSSQL)	Beachell (VM)	Upstream dependency – Bellamy, POA Dashboard, OCCMS, Great Plains
	Application Services (Bellamy)	Insert server name	
	Application Services (POA Dashboard)	Insert server name	
	Application Services (Great Plains)	Insert server name	
	Application Services (OCCMS)	Insert server name	
	Application Services (Council Express)	Insert server name	

Application/Server to Database Mapping	
Server Name	Database Type
Beachell	Microsoft SQL Server
McDonald	PostgreSQL
Lantz	MariaDB

Application Service	Database Type
ECM (Alfresco)	PostgreSQL
GIS	Microsoft SQL Server
Great Plains	Microsoft SQL Server
POA Dashboard	PostgreSQL
Corporate Website	MariaDB
OCCMS	Microsoft SQL Server
SRM HRWare	Microsoft SQL Server
CAMS	Microsoft SQL Server
Inspections Reporting	Microsoft SQL Server
Worksheets	PostgreSQL
Tweedsmuir Web Service	PostgreSQL
WSIB	PostgreSQL
Capital Projects	Microsoft SQL Server
Emergency Contacts	PostgreSQL
Emergency Management Portal	PostgreSQL
Bellamy	Microsoft SQL Server
Permit Payments	MariaDB
Council Meeting Management	PostgreSQL

Figure 2 - Application/Server Mapping

Plan Maintenance and Testing

While efforts will be made initially to construct this DRP is 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

Grey County 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.