Perry Group Consulting Ltd.

Business Continuity/ Disaster Recovery Program

Disaster Recovery Invocation Guide

County of Middlesex

Authors: Gary Walker, Brian Whitelaw, Perry Group Consulting

vDRAFT

encase™

INSTRUCTIONS

The IT **DR Invocation Guide** outlines the objectives of the overarching disaster recovery strategy and includes the following:

- **Policy Statement** – approach for safeguarding the vital technology and data managed by the County's Information Technology (IT) Department.
- **Staffing Requirements/Notification Process** – definition of County roles and responsibilities, DR call tree, and invocation guidelines.
- **Critical Asset List/Access Control** – use this document to add details on critical technology assets and staff authorization to access County datacenter facilities.
- **Current Posture** – Use this document to detail the County's current DR posture including backup/recovery procedures.
- **Impact Analysis Summary** – this section includes a summary of critical services and County response strategy.

Contents

TERMS AND DEFINITIONS 5

INTRODUCTION 8

STATEMENT OF INTENT 10

POLICY STATEMENT 10

OBJECTIVES 10

STAFFING REQUIREMENTS 11

INCIDENT RESPONSE TEAM (IRT) 12

CRISIS MANAGEMENT TEAM (CMT) 12

IT DISASTER RECOVERY TEAM & BUSINESS RECOVERY TEAM 12

NOTIFICATION CALLING TREE 14

..... 14

INFRASTRUCTURE OVERVIEW 15

IT CRITICAL ASSET LIST 15

DATA CENTER ACCESS CONTROL 16

NETWORK TOPOLOGY 17

BACKUP AND RECOVERY PROCEDURES 18

DISASTER RECOVERY CAPABILITIES 18

BUSINESS IMPACT ANALYSIS 19

CRITICAL IT SERVICES 19

IMPACTS AND SCENARIOS – TECHNICAL APPROACH 22

RESPONSE STRATEGY 22

APPENDIX A – SAMPLE IT CONTINUITY, BACKUP AND RECOVERY POLICY 26

APPENDIX B – IT INCIDENT PROCESS FLOW 33

Document Control

Document creation and edit records should be maintained by the County's disaster recovery coordinator (DRC) or business continuity manager (BCM).

Document Name	
Version	
Date Created	
Date Last Modified	
Last Modified By	

Document Change History

Version	Date	Description	Approval

TERMS AND DEFINITIONS

Term	Definition
Alternate Site	A site held in readiness for use during/following an invocation of business or disaster recovery plans to continue urgent and important activities of an organization.
Application Recovery	The component of Disaster Recovery that deals specifically with the restoration of business system software and data after the processing platform has been restored or replaced.
Business Continuity	The strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level. The capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident.
Business Continuity Management (BCM)	Holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.
Business Continuity Plan (BCP)	Documented procedures that guide organizations to respond, recover, resume and restore to a pre-defined level of operation following disruption.
Business Impact Analysis (BIA)	Process of analyzing activities and the effect that a business disruption might have on them.
Business Interruption	Any event, whether anticipated (i.e., public service strike) or unanticipated (i.e., blackout) which disrupts the normal course of business operations at an organization's location.
Call Tree	A document that graphically depicts the calling responsibilities and the calling order used to contact management, employees, customers, vendors, and other key contacts in the event of an emergency, disaster, or severe outage situation.
Crisis Management	The overall direction of an organization's response to a disruptive event, in an effective, timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation, and ability to operate. Development and application of the organizational capability to deal with a crisis.
Datacenter Recovery	The component of disaster recovery which deals with the restoration of data center services and computer processing capabilities at an alternate location and the migration back to the production site.
Declaration (DR)	A formal announcement by pre-authorized personnel that a disaster or severe outage is predicted or has occurred and that triggers pre-arranged response and mitigating actions.
Disaster Declaration	The staff should be familiar with the list of assessment criteria of an incident versus disaster situation established by the BCM or DR Steering Committee and the notification procedure when a disaster occurs.

Term	Definition
Disaster Recovery Plan (DRP)	The management approved document that defines the resources, actions, tasks and data required to manage the technology recovery effort.
Emergency Operations Center (EOC)	The physical location at which the coordination of information and resources to support incident management (on-scene operations) activities normally takes place. The facility used by the Incident or Crisis Management Team after the first phase of a plan invocation. An organization must have a primary and secondary location for an EOC in the event of one being unavailable. It may also serve as a reporting point for deliveries, services, press and all external contacts.
Incident	An event which is not part of standard business operations which may impact or interrupt services and, in some cases, may lead to disaster. Situation that might be, or could lead to, a disruption, loss, emergency or crisis.
ITIL	A set of detailed practices for IT service management that focuses on aligning IT services with the needs of business.
IT Service Continuity Management (ITSCM)	Aims to manage risks that could seriously impact IT services. This is an ITIL process that ensures the IT service provider(s) can always provide minimum agreed Service Levels, by reducing the risk from disaster events to an acceptable level and planning for the recovery of IT services. ITSCM should be designed to support Business Continuity Management.
Maximum Tolerable Downtime (MTD)	Time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable.
Qualitative Risk Assessment	The process for evaluating a business function based on observations and does not involve measures or numbers. Instead, it uses descriptive categories (e.g., customer service, regulatory requirements)
Quantitative Risk Assessment	The process for placing value on a business function for risk purposes. It is a systematic method that evaluates possible financial impact for losing the ability to perform a business function. It uses numeric values to allow for prioritizations.
Recovery Point Objective	The point in time to which data is restored and/or systems are recovered after an outage. The point to which information used by an activity must be restored to enable the activity to operate on resumption.
Recovery Time Objective	The period of time within which systems, applications, or functions must be recovered after an outage. RTO includes the time required for: assessment, execution and verification. The period of time following an incident within which a product or service or an activity must be resumed, or resources must be recovered.
Risk Acceptance	A management decision to take no action to mitigate the impact of a particular risk.
Risk Analysis	The quantification of threats to an organization and the probability of them being realized.

Term	Definition
Risk Appetite	Total amount of risk that an organization is prepared to accept, tolerate, or be exposed to at any point in time.
Risk Assessment	Overall process of risk identification, risk analysis, and risk evaluation.
Risk Mitigation	Implementation of measures to deter specific threats to the continuity of business operations, and/or respond to any occurrence of such threats in a timely and appropriate manner. Activities taken to reduce the severity or consequences of an emergency.
Risk Register	All risks of an organization, listed, ranked and categorized so that appropriate treatments can be assigned to them.
Single Point of Failure	A unique pathway or source of a service, activity, and/or process. Typically, there is no alternative and a loss of that element could lead to a failure of a critical function. Unique (single) source or pathway of a service, activity and/or process; typically there is no alternative, and loss of that element could lead to total failure of a mission critical activity and/or dependency.
Tabletop Exercise	Technique for rehearsing teams in which participants review and discuss the actions they would take according to their plans, but do not perform any of these actions.
Vital Records	Records essential to the continued functioning or reconstitution of an organization during and after an emergency and also those records essential to protecting the legal and financial rights of that organization and of the individuals directly affected by its activities.

INTRODUCTION

Emergency preparedness, business continuity, crisis response, disaster recovery: These and other related terms are often discussed as if they are synonyms that all refer to the process of responding to and mitigating a crisis event. However, they provide very different business functions and it's particularly important for the County to document and communicate the differences between **emergency preparedness** and **business continuity** throughout the organization in order to establish correct accountability for each discipline.

A clear distinction should be made between emergencies, crises and disasters in order to develop and provide appropriate response plans. However, what may begin as a small routine emergency may turn into a major crisis or a major disaster. Conversely, not all emergencies end up being a crisis. It would all depend on the timing, nature and surrounding context of the event.

Emergency Preparedness: typically involves directing people and resources away from danger, holding emergency drills and training sessions, evacuating facilities and working with first responders to ensure the health and safety of all stakeholders.

Business Continuity: involves protecting the business' reputation, establishing and maintaining redundant systems and support teams, restoring IT systems and ensuring employees are able to return to their daily work tasks following an emergency.

Of course, despite the differences between emergency management and business continuity, in the end these two distinct departments are both working toward the same objective: to help ensure the success of the business.

The County currently has an **Emergency Operational Centre** team of approximately fifteen staff members with clearly defined roles and responsibilities. In the ideal corporate set-up, emergency management and business continuity personnel would be completely separate entities with their own teams. The County will need to review this further in order to determine the ideal structure.

The scope of this document pertains to the County's IT service continuity strategy; a subset of business continuity management (BCM). Often referred to as "DR", IT service continuity management "ITSCM" is focused on planning for the restoration of IT-based services and technologies. ITSCM addresses the gaps in the traditional disaster recovery approach by introducing layers of resilience that provide higher levels of protection. This layering is realized by using technologies that are readily available such as virtualization and high availability fail over. This approach aligns with ITIL best practices.

Aligning ITIL processes to the County's DR plan will lead to more efficient and effective use of IT infrastructure. Inadequate planning is a risk to the business and is often overlooked until it is too late, when a crisis event such as a major infrastructure outage, security or other breach results in the loss of supporting IT systems.

Recovery options need to be considered for IT systems and networks, and critical services such as telecommunications and power. The various recovery options are as follows:

- **Do nothing** - However, few organizations can afford to forgo all business activities supported by IT services and simply wait until services are restored.
- **Manual system** - For businesses without a large number of critical IT services, manual workarounds may present a feasible option until IT services can resume.

- **Reciprocal arrangement** - This option involves forming an arrangement with another company that uses similar technology.
- **Gradual recovery** - This option is often chosen by organizations have certain business services supported by IT that are not required for 72 hours or longer.
- **Warm start** - This is an option used by organizations that need to recover IT services and facilities within a 24- to 72-hour period. To accomplish this, organizations often use commercial facilities that include operations, system management, and technical support.
- **Hot start** - This is also known as an immediate recovery. This option is used for critical services that cannot be down for any length of time. A hot start provides for immediate restoration of IT services. It is also one of the most expensive options to implement.

Common problems associated with ITSCM are issues that prevent an organization from committing to continuity management - in terms of both implementing the process and maintaining it. One example is when organizations seem unable to move out of the planning stage and into actual implementation.

Other examples are being unable to find facilities or resources, having someone unfamiliar with the business implement the process, not understanding ITSCM's role in disaster recovery, or thinking IT has already handled continuity planning.

Common costs associated with ITSCM are the expenses incurred from risk management and recovery arrangements. An example of a common cost is the investment required by the introduction of risk management.

Additional examples of common costs are returning operational costs and the hardware needed to support the ITSCM process, and fees for the recovery facility. There will always be problems and costs associated with implementing ITSCM. But the resulting benefits, especially when a disaster is prevented or quickly controlled, outweigh the associated difficulties and costs.

This document provides policies and guidance to be used by the County's **Information Technology** group to carry out responsibilities under ITSCM for information systems security and availability regarding system contingency plans and recovery after a disruption or disaster.

Statement of Intent

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

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

Policy Statement

- County of Middlesex 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.

Please refer to Appendix A – Sample IT Continuity, Backup and Recovery Policy for a recommended approach to IT continuity, backup, and recovery.

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 staff 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 County sites; and
5. Disaster recovery capabilities as applicable to key customers, vendors and others.

STAFFING REQUIREMENTS

No DR initiative can ever work without people. County staff will constitute part of the resources and capabilities required to deliver a quality recovery strategy to users and customer alike. And since quality service delivery is all about dealing with customers, users and suppliers, the value of instituting proper roles and responsibilities in within the DRP cannot be understated.

Since Disaster Recovery falls within the scope of Business Continuity Management (BCM), it's important to highlight the keys areas of disciple that require well-define roles and responsibilities. Depending on the size of an organization, the number and size of these teams will vary.

The primary objective of this document is to address the need to develop a disaster recovery team structure as highlighted in red in *figure1,* however ancillary teams to support incident management, crisis management, and business continuity will be covered at a high-level.

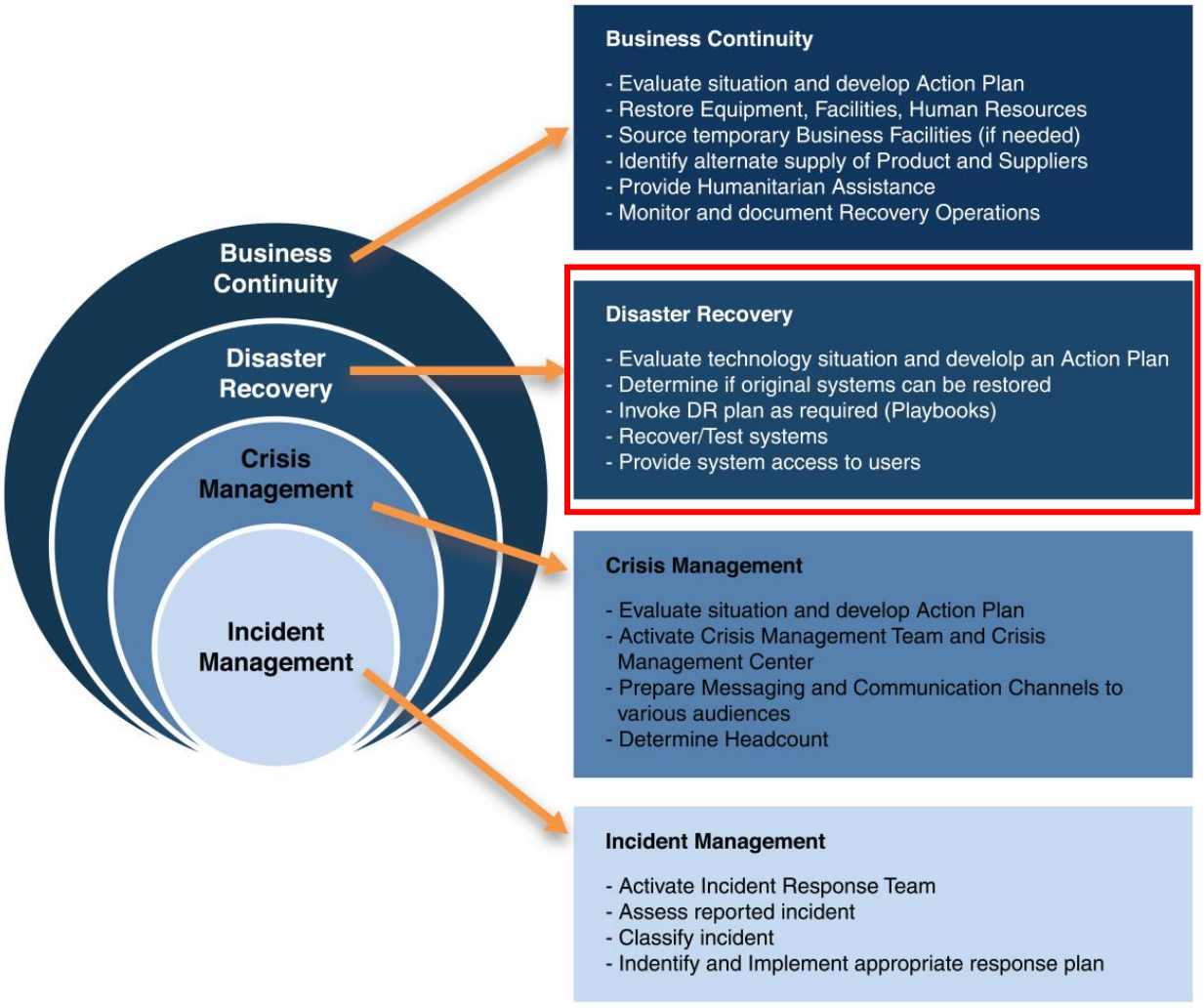


Figure 1 - Business Continuity Management

Incident Response Team (IRT)

Incident response can be considered as the “entry” to IT service continuity management (ITSCM). As it relates to technology, Incident response relies on the Service Desk personnel and decisions/classification capabilities defined by Incident Management. A decision must be made to decide if ITSCM contingencies and capabilities should be used, and when the trigger should be pulled after a disruption (based on senior management decisions). The ITSCM process is accountable for ensuring all knowledge, information, and documentation is available to the IM team for making informed recovery invocation decisions.

Note that the IRT referred to in this DR document may not be the same IRT specified in the County’s Security Incident Response Plan.

Refer to Appendix B – IT Incident Process Flow for details

Crisis Management Team (CMT)

The County should budget for the development of departmental business continuity plans. However, this is a time-consuming process that will require funding and County resources.

The single most cost-effective step the County can take is to involve senior management in the process of a response to crises. We recommend establishing a CMT with five or seven members so: there cannot be any “split-votes” in a crisis. Every division or business line does not need to be represented. The County should select decision-makers with a broad perspective on the business priorities. The CMT should include representatives from information technology, human resources, corporate communications, and facilities.

Note: Emergency Management (life safety) and Business Continuity (continuity of business operations) are two distinct disciplines that operate as separate groups although the emergency management team would report to the crisis management team if there was a "crisis".

Crisis Management will help to protect the County against situations that may have a negative effect on business operations and reputation (part of business continuity management).

The Crisis Management Team would typically be led by senior leadership with authority to invoke something like the IT disaster recovery plan or business continuity plans.

IT Disaster Recovery Team & Business Recovery Team

At a minimum a DR coordinator should be in place and responsible for:

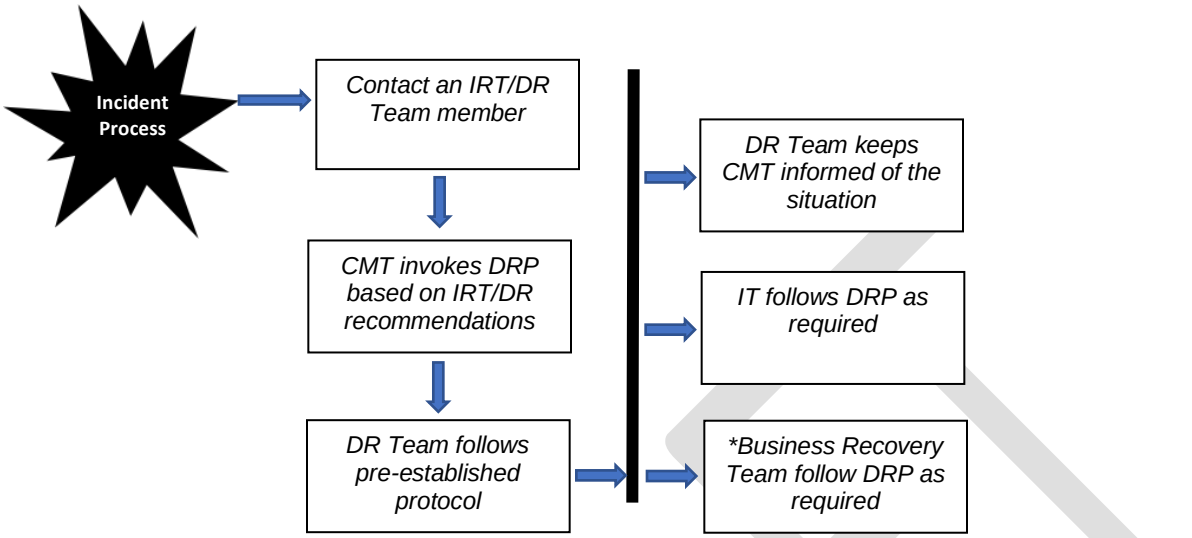
- establishing ITSC plans to provide agreed-on levels of service within agreed timelines following a disruption/disaster;
- ensuring that IT service areas are able to respond to an invocation of the continuity plans;
- maintaining a comprehensive IT testing schedule and undertaking regular reviews; and
- selecting the appropriate business recovery team(s) at time of disruption/disaster to assist in the recovery/testing of critical business applications.

Additional roles will include recovery team members from the infrastructure team to cover the network, servers, storage, databases, and telecommunications.

Note: In considering the size of the IT department, the recommendation is to consolidate the Incident Response (IR) and IT Disaster Recovery (DR) teams with 5-7 members within the IT department.

NOTIFICATION CALLING TREE

In the event that a full/partial DR has been declared by the CMT *after* the initial assessment by the Incident Response team, the following call tree should be used to coordinate system recovery:



*Contact Departmental Leads as Required

In the event of a disaster recovery invocation please refer to the following supplementary documents:

Disaster Recovery Plan Activation Form – this form contains up to date activation steps, order of restoration, and contact lists.

Disaster Recovery Event Recording Form – this form is to be completed by the disaster recovery team leader once the infrastructure has been recovered and all required applications

Business Resumption Form (Application Recovery) – a copy of this form should be completed with sign-off by the business recovery lead and the designated lead for each department for all applications recovered during the disruption.

System Recovery Run Books – this document includes a template to be used in the development of system recovery run books for all required County systems.

INFRASTRUCTURE OVERVIEW

IT CRITICAL ASSET LIST

IT assets are considered “critical” if they are supporting the delivery of Tier 1-3 services/processes. The following list has been identified through the BIA process:

Table 1 - Critical IT Asset List

Critical IT Asset List
This list captures all IT assets required to support business processes/services with recovery time objective (RTO) ranging from 0-3 days.

Asset	Type/Sub-Type	Location	Description/Notes

DATA CENTER ACCESS CONTROL

Table 2 - Data Centre Access Control List

Data Center Access Control List

Maintain an up-to-date access control list (ACL) specifying who, within the County and any service partners, has access to the data center and resources herein.

Be sure to specify which individuals can introduce guests to the data center. This is required for determining, in the event of an emergency, who may be the designated point person for facilitating access to critical infrastructure. During a recovery event, the County's primary operations team will be involved in system recovery, making contact and data center access information critical to the success of the recovery process.

Name	Role	Contact Info	Access Level

NETWORK TOPOLOGY

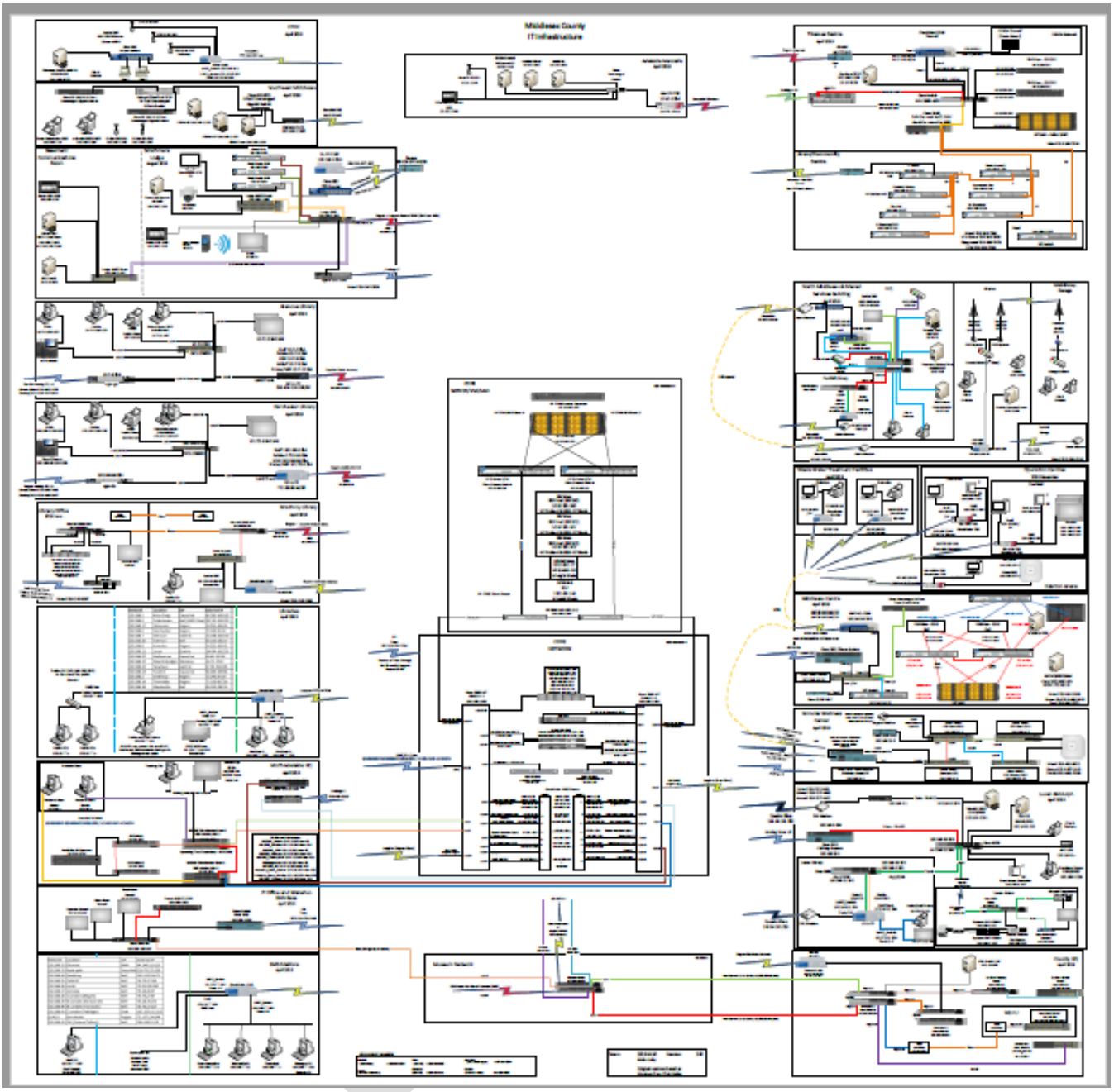


Figure 2 - IT Network Topology

Backup and Recovery Procedures

The County has backups schedules as follows:

- Incremental Backups occur from Monday to Friday outside of Regular Business Hours (User files and Unstructured Data)
- A Full Backup is taken on the first Saturday of each month outside of Regular Business Hours
- Backup to Removable Media occurs each Sunday
- Backups will be written to Removable Media each Sunday and stored off-site by a trusted third-party company
    - Removable Media backups will be picked up each Monday
- A minimum of 30 days of backup files will be available on-site for restoration purposes
- To ensure the availability of data, each Full Backup will be kept off-site for a minimum of 1 year on Removable Media

Disaster Recovery Capabilities

The County last had a DR planning exercise in 2008. A report provided by a third-party was received, with some of the ideas implemented. Since then, most recovery capabilities are based on a robust backup schedule and process….

Capabilities (DR site)

- While there is no DR site as such, there is a robust core infrastructure using multiple VMware ESX hosts incorporating high availability, along with other core network redundancy, including a 3 node HP SAN (Storage Area Network). When coupling this with the backup schedules, the County has some DR capabilities under certain circumstances.

Limitations (DR site)

- While recognizing the robust core network and backups schedules, the County does not have true DR capabilities, leaving it vulnerable to major issues within the data centre or even at the County Building.

BUSINESS IMPACT ANALYSIS

CRITICAL IT SERVICES

Table 7 below delineates IT services required to support critical County services as defined in the business impact analysis. For the purposes of this document, ONLY services categorized as **Tier 1-4** will be identified.

These services have been categorized as follows:

Table 3 - Critical IT Services

	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5 (NA)
RTO Legend:	0-4 hours	24-hours	3-days	7-days	2-4 weeks

IT Service Breakdown by Criticality		
IT Service	Service/Process Dependencies	RTO
Network Access	County Clerk (Reception) Legal Services (Advisement & Litigation) Legal Services (By-Law Prosecutions) Legal Services (Court Appearances) Legal Services (Negotiations/Business Advice) Long Term Care (Food Services) Long Term Care (Nursing) Paramedics (Critical Patient Transfers) Paramedics (Large Incident/Disaster Response) Paramedics (Paramedic Response) Roads (Emergency Management) Roads (Fire Dispatch/Radio) Social Services (Social Assistance Management System (SAMS) Treasury (Accounts Payable)	
Print/Fax Service	Legal Services (By-Law Prosecutions) Legal Services (Court Appearances) Paramedics (Large Incident/Disaster Response) Roads (Emergency Management) Social Services (Social Assistance Management System (SAMS) Treasury (Accounts Payable)	
Email	Legal Services (By-Law Prosecutions) Legal Services (Court Appearances) Legal Services (Negotiations/Business Advice) Long Term Care (Food Services) Long Term Care (Nursing) Paramedics (Large Incident/Disaster Response) Roads (Emergency Management) Roads (Fire Dispatch/Radio)	
Wireless Internet Services	Long Term Care (Nursing)	

Critical IT Servers (Continued)

	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5 (NA)
RTO Legend:	0-4 hours	24-hours	3-days	7-days	2-4 weeks

IT Service Breakdown by Criticality

IT Service	Service/Process Dependencies	RTO
Internet Services	Legal Services (By-Law Prosecutions) Legal Services (Court Appearances) Legal Services (Negotiations/Business Advice) Long Term Care (Food Services) Long Term Care (Nursing) Paramedics (Critical Patient Transfers) Paramedics (Large Incident/Disaster Response) Paramedics (Paramedic Response) Roads (Emergency Management) Roads (Fire Dispatch/Radio) Social Services (Social Assistance Management System (SAMS)	
File Services	Legal Services (Advisement & Litigation) Legal Services (By-Law Prosecutions) Legal Services (Court Appearances) Legal Services (Negotiations/Business Advice) Long Term Care (Food Services) Long Term Care (Nursing) Paramedics (Large Incident/Disaster Response) Roads (Emergency Management)	
Telephony (Desktop/VOIP)	County Clerk (Reception) Legal Services (By-Law Prosecutions) Long Term Care (Environmental Services) Long Term Care (Food Services) Long Term Care (Nursing) Paramedics (Critical Patient Transfers) Paramedics (Large Incident/Disaster Response) Paramedics (Paramedic Response) Roads (Emergency Management) Roads (Fire Dispatch/Radio) Social Services (Social Assistance Management System (SAMS)	
Telephony (Cellular)	Legal Services (Advisement & Litigation) Legal Services (Court Appearances) Legal Services (Negotiations/Business Advice) Paramedics (Critical Patient Transfers) Paramedics (Large Incident/Disaster Response) Paramedics (Paramedic Response) Roads (Emergency Management) Roads (Fire Dispatch/Radio)	

Critical IT Servers (Continued)

	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5 (NA)
RTO Legend:	0-4 hours	24-hours	3-days	7-days	2-4 weeks

IT Service Breakdown by Criticality

IT Service	Service/Process Dependencies	RTO
Application Services (FirePro)	Roads (Fire Dispatch/Radio)	
Application Services (First Watch)	Long Term Care (Nursing) Paramedics (Paramedic Response)	
Application Services (Great Plains)	Treasury (Accounts Payable)	
Application Services (Microsoft Office Suite)	Long Term Care (Nursing) Paramedics (Large Incident/Disaster Response)	
Application Services (ProLaw)	Legal Services (Advisement & Litigation) Legal Services (By-Law Prosecutions) Legal Services (Court Appearances) Legal Services (Negotiations/Business Advice)	
Application Services (SAMS)	Treasury (Accounts Payable) Social Services (Social Assistance Management System (SAMS)	
Website Hosting and Content Management	County Clerk (Agenda Preparation)	
Application Services (OMNIRIM)	County Clerk (MFIPPA Requests)	
Application Services (eGenda)	County Clerk (Agenda Preparation)	
Application Services (ESRI)	Planning (GIS Planning Local)	
Application Services (Laserfiche EDM)	Human Resources (Health & Safety)	
Application Services (Laserfich Forms)	County Clerk (Records Management)	

Impacts and Scenarios – Technical Approach

Business continuity planning has evolved over time and has expanded in scope of what it tries to achieve. Business Continuity Planning intertwines with Emergency Management and therefore includes both emergency response components and contingency planning components.

In considering these two components of the overall program, emergency response addresses how an organization responds to an incident and should, in fact, have scenario specific components for the known risks and threats in the area where you do business. If you have facilities in regions susceptible to ice storms, you absolutely should have Ice Storm Preparedness Plans.

When specific threats arise, like pandemics, for example, your organization should develop a scenario specific plan for prevention and contention techniques for that exact threat.

However, on the contingency side of things, the focus should be on the impact. Contingency plans should be developed based on impacts, such as: loss of access to the building; loss of access to technology tools, applications and data; interruptions in workflow; depleted or immobilized work force.

Response Strategy

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

1. County Data Center and Main County Building – 1035 Adelaide Street North and 399 Rideout Street North

SYSTEMS	**Core IT systems not available for >4 hours during working hours**
SERVICES	**No Connectivity available for >4 hours**
SITE	**Unable to access site for any period more than 4 business hours**

SYSTEMS	Core IT system(s) not available for >4 hours during working hours

Hardware Component Failure

Planned Response Strategy	Expected Response Results	Post-Disaster Expectations
Assess situation – restore systems on site if possible (as per run book) Contact Hardware vendor - identify if replacement can be procured before SLA's and RTOs have been infringed. If required, enable full/partial DR failover for systems affected.	100% of core infrastructure will available on site or at the DR site. 100% of Tier 1 applications and services will be available within 4 hours onsite or at the DR site. Tier 2-3 systems to be restored within 1-3 days respectively.	DR site will be restored to production systems (failback). Build more hardware redundancy if required.

Software Failure

Planned Response Strategy	*Expected Response Results*	*Post-Disaster Expectations*
Assess situation – restore systems onsite if possible (as per run book). Contact software vendor or in-house developer for support, upgrades, revisions or patches. Restore last known working version of the software stack. If required, enable full/partial DR failover for systems affected.	100% of core infrastructure will available onsite or at the DR site 100% of Tier 1 applications and services will be available within 4 hours on site or at the DR site. Tier 2-3 systems to be restored within 1-3 days respectively.	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- Identify the systems affected. Take appropriate action, permissions, take offline. Eliminate security breach. Restore systems on site if possible (as per run book). If required, enable full/partial DR failover for systems affected.	**Security breach must be closed before activating redundant DR systems.** 100% of core infrastructure will available onsite or at the DR site. 100% of Tier 1 applications and services will be available within 4 hours onsite 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 - Identify the systems affected. Take appropriate action, update virus definition, patch and deploy if required. Restore systems on site if possible (as per appropriate run book(s)). If required, enable full/partial DR failover for systems affected.	**Virus incident must be eliminated or isolated before activating redundant DR systems.** 100% of core infrastructure will available onsite or at the DR site. 100% of Tier 1 applications and services will be available within 4 hours onsite 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 - Restore data from archives (as per appropriate run book(s)). If required, enable full/partial DR failover for systems affected.	100% of core infrastructure will be available onsite or at the DR site. 100% of Tier 1 applications and services will be available within 4 hours onsite 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 - Restore systems from backups (as per appropriate run book(s)). If required, enable full/partial DR failover for systems affected.	Eliminate error; ensure there is no replication to DR systems. 100% of core infrastructure will be available onsite or at the DR site. 100% of Tier 1 applications and services will be available within 4 hours onsite 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 in local issue, 1 hour if within premises 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 DRP if required for systems affected. Contact provider for immediate engineer investigation – 4 hour SLA expected for resolution Move staff if appropriate. Restore systems onsite if possible.	100% of core infrastructure will be available onsite or at the DR site 100% of Tier 1 applications and services will be available within 4 hours onsite or at the DR site - backup system in place.	Once the Network is again accessible, restore to production systems.

SITE	Unable to access site for any period more than 4 business hours	
County Building Cannot be Accessed		
Planned Response Strategy	**Expected Response Results**	**Post-Disaster Expectations**
Assess situation then enable DRP if required for systems affected (as per appropriate run book(s)). *e.g. Structural Failure, Power Failure, Water Damage, Fire,* Move staff as and if appropriate.	100% of all core infrastructure will be available immediately at DR Site 100% of Tier 1 applications and services will be available within 4 hours at DR site. Tier 2-3 systems to be restored within 1-3 days respectively.	Once the County Building is again accessible, restore to production systems (failback).

APPENDIX A – SAMPLE IT CONTINUITY, BACKUP AND RECOVERY POLICY

Policy Statement

The County of Middlesex technology infrastructure supports a variety of business applications used in the process of delivering services to residents, businesses and internal clients. Effective recovery plans are in place to ensure that IT services can be resumed within required recovery times in the event of a system disruption or disaster.

Background

A disruption, loss, damage or compromise of IT systems and data may negatively impact the County reputation and operations, resulting in significant costs to recover. Formal and comprehensive IT continuity, backup and recovery controls are necessary to mitigate such risks.

Policy Objective

The objective of this policy is to define formal requirements for IT continuity, backup and recovery, in order to prevent or mitigate the risk of IT system disruption or disaster and allow for an efficient recovery of IT services and data in a timely manner.

Scope

This policy applies to all IT systems or applications managed by the IT Department that store, process or transmit information, including network and computer hardware, software and applications.

This policy does not apply to information that is stored locally by users on desktops, laptops, tablets and mobile phones. Device owners are responsible for appropriate backup of the data stored locally on their mobile devices, with the exception of data synchronized with the device and stored on IT servers (such as Outlook emails and contacts).

Definitions

A BCP “Business Continuity Plan” is a comprehensive plan describing the strategy and necessary activities to recover from a significant disruption of business operations, including by relocating part or all personnel and system resources, making urgent decisions, and conducting business operations with diminished or altered capabilities.

A DRP “Disaster Recovery Plan” is a documented set of procedures describing the key activities that are necessary to recover minimum IT services, applications and data to continue critical business operations, and to fully recover such operations after a disaster affecting normal IT services.. Effective recovery plans are in place to ensure that IT services can be resumed within required recovery times in the event of a system disruption or disaster.

A RTO “Recovery Time Objective” refers to the maximum tolerable length of time that a computer, system, network, or application can be down after a failure or disaster occurs.

Guiding Principles

IT systems that are critical to Institution activities must be clearly identified, as well as the potential risks of disruption that apply to them.

IT continuity, backup and recovery must be managed in accordance with:

- The Emergency Response and Business Resumption Policy.

- Guidelines contained in Appendix 1 of this policy.

Recovery Time Objectives ("RTOs") of critical systems must be formally defined as per the business needs.

Procedures and technology must be in place and tested regularly to ensure:

- Prevention against IT system disruption.
- Regular and comprehensive backup of critical systems, applications and data.
- Timely recovery of critical systems, in line with the business expectation or RTO.

Roles and Responsibilities

Stakeholder	Responsibility
TBD (CAO?)	Approve and formally support this Policy
TBD (Department Heads?)	Review and formally support this Policy
IT Director	• Develop and maintain this Policy. • Review and approve any exceptions to the requirements of this Policy. • Take proactive steps to reinforce compliance of all stakeholders with this Policy. • Communicate with the Institution, directly or through Institution representatives, in informal or formal instances, to understand the Institution needs and expectations, explain the capabilities of the existing technology in production, including backup and recovery capabilities

Exceptions to the Policy

Exceptions to the guiding principles in this policy must be documented and formally approved by the IT Director.

Policy exceptions must describe:

- The nature of the exception
- A reasonable explanation for why the policy exception is required
- Any risks created by the policy exception
- Evidence of approval by the IT Director

Inquiries

Inquiries regarding this policy can be directed to the IT Director.

Amendments (Revision History)

Amendments to this policy will be published from time to time and circulated to the Institution community.

Appendix 1 - IT DRP and Backup Guidelines

IT Disaster Recovery

An IT Disaster Recovery Plan (IT DRP) must be formally documented and contain the following details:

1. Step-by-step procedures to recover critical IT systems and applications and restore data after a major disruption, including:
    a. Emergency response to a major disruption;
    b. Initial recovery of the most critical IT systems;
    c. Full recovery of most critical systems, applications and data at a level defined in the business impact analysis; and
    d. Return to a normal situation.
2. Clear roles and responsibilities.
3. List of critical systems and applications that are aligned with the BCP.
4. Detailed minimum requirements and specifications for the critical IT system components, including mapping of critical applications and data hosted on servers.
5. Contact information of key resources, including phone numbers (daytime and nonworking hours), email and physical address where possible, for:
    a. The IT DR team.
    b. Other IT contacts (IT staff, 3rd party IT supplier, application vendors, etc.).
    c. Other business contacts (applications and system owners and administrators, key suppliers, customers and stakeholders, communication team, etc.).
6. The IT DRP plan must be reviewed and tested at least annually to ensure documented information is up to date and that all team members are aware of their responsibilities, roles and tasks to roll-out the plan effectively.
7. Regular tests of the IT DRP may include the following:
    a. High-level plan walkthrough
    b. Table top exercise
    c. Simulation exercise
    d. Test of the communication channels and call notification procedures
    e. Data backup restoration
8. A copy of the IT DRP plan must be available off-site (using a laptop for example).

Preventative Requirements

1. Protection from power failures or other electrical anomalies must be in place, including where possible:
    a. Multiple power feeds or power supplies
    b. Uninterruptible Power Supplies (UPS) with sufficient running time for:
        i. Switching to an alternative source of power
        ii. Backing-up IT systems or transferring data

iii. Clean shut down of all IT systems. If equipment supporting critical business operations is not capable of auto-shutdown, then the equipment shall be powered down in accordance with an emergency shutdown procedure.

c. Back-up generators or other source of alternate/secondary power.
d. All power to critical IT infrastructure shall be filtered to provide a source of "clean" power.
e. All power supply equipment must be maintained, regularly checked and tested in accordance with the manufacturer's recommended instructions or procedures.
f. Surge protection shall be installed, wherever possible, to all buildings housing critical IT processing or infrastructure equipment.

2. Protection from environmental hazards must be in place, including where possible:
   a. Hazardous or combustible materials shall not be stored within data centers or data-rooms.
   b. Appropriate equipment must be installed in data centers or data-rooms to monitor and react to fire, flood, high temperature, vibration, air quality and dust hazards.
3. Systems redundancy and high-availability equipment must be in place where appropriate.

Backup Procedures

Generic Backup Requirements:

1. Contingency IT equipment must be in place where appropriate.
2. Backups of critical systems must cover system files, software files and data files, for both the running systems and the default system-built image.
3. A combination of backup technology must be used to ensure the most efficient backup and recovery of operation services. Automated backups must be performed including one of the following solutions:
   a. Network-Attached Storage (NAS)
   b. Direct-Attached Storage (DAS)
   c. Storage Area Network (SAN)
   d. Replication and mirroring technologies
   e. Backup management system, backup tapes and tape libraries
4. Different backup media must be used and retained for each backup type (i.e. daily, weekly, monthly, or any other defined period).
   a. Further, to ensure greater integrity of the backups, distinct backup media pools must be used where possible.
5. A Backup Coordinator must be designated with the responsibility of managing, operating, and troubleshooting backup solutions, as well as answering any requests related to backups and recoveries.
6. Quality and integrity of backups must be verified at the end of each backup operation.
7. Backup systems must be configured to automatically generate email alerts, warnings and status updates to the Backup Coordinator where possible.

Backup Frequency and Retention

The County has backups schedules as follows:

- Incremental Backups occur from Monday to Friday outside of Regular Business Hours (User files and Unstructured Data)
- A Full Backup is taken on the first Saturday of each month outside of Regular Business Hours
- Backup to Removable Media occurs each Sunday
- Backups will be written to Removable Media each Sunday and stored off-site by a trusted third-party company
    - Removable Media backups will be picked up each Monday
- A minimum of 30 days of backup files will be available on-site for restoration purposes
- To ensure the availability of data, each Full Backup will be kept off-site for a minimum of 1 year on Removable Media

Physical security of backup media and contingency IT equipment

1. Fallback or contingency equipment and backup media stored off-site must be at a sufficient distance to escape any damage from a disaster at the main site.
2. Long-term storage of backup data must meet the same basic physical and environmental control requirements in place for the critical IT systems in production.
3. Appropriate care of all backup media must be taken to preserve their integrity. Specifically, tapes must be stored according to the vendor recommendations and must not be exposed to sources of contamination, such as copiers and printers (that emit toner and paper dust), or high voltage electrical equipment (that emit electromagnetic radiation damageable to magnetic tapes).
4. Backup media reaching the end of their retention period, must be fully erased and recycled in the pool of available backup media.
5. Any damaged, corrupted or end of life tapes must be destroyed.
6. All backup media must be labelled and identified with a unique identifier.
7. A detailed inventory must be maintained at all times to track the position and status of all backup media. The use of an automated inventory system is acceptable but must be completed with regular verification of the true position and status of backup media.
8. Every physical transfer of backup media off-site must be formally tracked with the following criteria:
    a. Date and time of transfer.
    b. Origin and destination locations.
    c. Name of the person and organization taking the responsibility of the transfer.
    d. Detailed inventory of the media being transferred.
    e. Backup media stored off-site must be encrypted; where this is not possible, mitigating controls should be considered.
    f. Security controls must be implemented to prevent access to backup management systems, backup files and backup media, including:
        i. Physical and logical access restriction based on the user role and responsibilities.

ii. Changing all default login and passwords.

iii. Logging of: system access; changes to system configuration, system files and user access rights; and access to the log files.

Recovery

Standard Restoration Process

1. All restore requests must be formally submitted to the IT Help Desk, who will sequence and address the request to the Backup Coordinator. Requests must detail the following:
   a. Specific file(s) and / or folder(s) that are required to be restored.
   b. From which server.
   c. From which specific date.
   d. To what restore location.
   e. Whether the restored data should over-write the current data in the original location (or not).
2. A detailed procedure for data restoration must be documented, including the restoration of data stored in both on-site and off-site backups.

Emergency Restoration Process

1. Emergency restoration must be formally approved by the IT Director.
2. Due care must be followed to prevent any loss of data or damage to backup media in an emergency.
3. Details of the backup restoration must be formally documented by the Backup Coordinator, after the emergency

Roles and Responsibilities – Procedures

Stakeholder	Responsibility
IT Director	• Develop and maintain this Policy. • Review and approve any exceptions to the requirements of this Policy. • Take proactive steps to reinforce compliance of all stakeholders with this Policy. • Communicate with the County staff, directly or through representatives, in informal or formal instances, to understand the County needs and expectations, explain the capabilities of the existing technology in production, including backup and recovery capabilities. • Formally approve the backup and recovery policy. • Formally approve the IT DRP.
Backup Coordinator	• Ensure tools used for backup and recovery are configured as per this Policy. • Ensure backups and recoveries are performed without issue and remediate any such issue.

Stakeholder	Responsibility
	• Answer and address requests to backup or to restore backed-up data or systems. • Provide recommendations regarding the processes to backup and recover IT systems, applications and data, and participate in the development of the BCP and the IT DRP. • Provide recommendations to improve or update this Policy.
System Owners	• Identify the critical IT systems, applications and data necessary to support critical business operations. • Define the minimum availability requirements for their systems, including Recovery Time Objectives (RTOs). • Participate in the development of the BCP and the IT DRP.
Division/Department Managers	• Participate in the development of the BCP and the IT DRP. • Communicate with the IT group for any need, concern or question related to IT systems availability, IT backup and recovery services
Users	• Contact the Help Desk/Service Desk for any question or concern related to the technology. • When a question or concern cannot be addressed by the Help Desk/Service Desk, contact their supervisor or representative. • Store all corporate files on network drives.

APPENDIX B – IT INCIDENT PROCESS FLOW