SECTION: Administration	**POLICY #: ADM-018**
Date Approved: May 6, 2019	**Information Systems Disaster Recovery (DR) & Business Continuity Plan**
Revision Date:	**Review Date: April 29, 2019**
Authority: Report DCS-11-19	

1.0 PURPOSE

The purpose of this policy is to establish processes to ensure the availability of all information systems required for essential business operations in the event of an equipment failure, service disruption or a loss of operational capacity resulting from a fire or natural disaster. The processes within this policy will ensure that those assets are recoverable to the right level and within the right timeframe to deliver a return to normal operations with minimal impact on the business.

2.0 SCOPE

This policy applies to the following services:

- Hanover Civic Centre Data Centre
- Microsoft File Services
- Microsoft Active Directory
- Microsoft Exchange Server
- Microsoft SQL Server

3.0 DEFINITIONS

Information system is defined as a system that is required to process information used in business operations. An information system includes all of the hardware, operating system software, application software, network connections and external services required for proper operations.

Backup Location is defined as a physical location that is geographically distant from the production location such that no single weather-related or other disaster would be likely to affect both locations.

Cloud is defined as a collection of hardware and software that is located in a secure location with redundant systems for power and internet connectivity. Public clouds are multi-tenant data centers where computing infrastructure can be purchased at a required capacity, on either a temporary or permanent basis.

Restore Point Objective (RPO) is the maximum targeted period in which data might be lost from an IT service due to a major incident.

Restore Time Objective (RTO) is the targeted duration of time in which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences.

Retention Policy is defined as a process for determining how long data restore points should be retained, and/or when they should be consolidated into less frequent restore points.

4.0 BACK-UP PROCESSES

Service RPO and RTO Targets

IT Service	Scenario	RPO	RTO	Priority
Email Systems	Server Failure	24 hours	4 hours	Medium
Active Directory	Server Failure	24 hours	4 hours	High
Exchanger Server	Server Failure	24 hours	4 hours	High
File Server	Server Failure	24 hours	4 hours	Medium
SQL Server	Server Failure	24 hours	4 hours	Low
Terminal Services	Server Failure	24 hours	4 hours	Low
FirePro	Server Failure	24 hours	4 hours	Medium
Any Above	Complete loss due to disaster	48 hours	24 hours	Medium

Backup Strategy

The retention of the restore points for all servers are backed up hourly for the first 5 days; reduced to once daily for the previous 23 days; reduced to weekly for the prior one week and then reduced to monthly prior to that up to a maximum of six months locally and up to one year storage of back-ups in the cloud.

IT Service	Backup Location	Backup Frequency
Exchange Server	Datto & Cloud	Hourly
File Server	Datto & Cloud	Hourly
SQL Server	Datto & Cloud	Hourly
Active Directory	Datto & Cloud	Hourly
Terminal Services	Datto & Cloud	Hourly
Fire Pro	Datto & Cloud	Hourly

The following servers are backed up to a Datto Siris SB2000.

- HAN-S01 (File, D, DHCP, DNS, print)
- HAN-S02 (Exchange email)
- HAN-S03 (Terminal services, WSUS, ePO, FirePro)
- HAN-S05 (SQL)

The Datto backup server creates image based backups of each server on an hourly basis. It has several operating modes that can provide continuation of services depending on the type of failure.

- **Local File Recovery** – An image can be mounted at any point in time in the backup chain that will allow access on a file level.
- **Local Virtualization –** An image can be mounted at any point in time in the backup chain and virtualized on the Datto server. This virtual server can be connected to the network and used during the time that the original server is down. Backups of the virtualized server will continue to happen on the Datto server.
- **Bare Metal Restore** - A repaired/replaced server can be restored directly from the Datto server to any point in time in the backup chain.
- **Virtualize in the Cloud** – An image can be mounted at any point in time in the offsite backup chain on the Datto cloud service and virtualized. A Virtual Private Network (VPN) connection can be made to this server from the local area network (LAN).

The Datto backup server automatically attempts to virtualize each server every day. This is a test to determine the quality of the current backup and ensure it functions as required. If the virtualization fails, an alert is sent to the Third Party IT Consultant provider.

Testing Schedule

- The Disaster Recovery (DR) will be tested in its entirety once every 6 months.
- Recovery process for IT services will be tested once every 6 months.

Plan Review

- The Disaster Recovery plan itself will be formally reviewed once every 6 months and in response to the regular testing.

5.0 DISASTER RECOVERY (DR) PROCESS

The following are to assume responsibility for restoring IT services when the disaster recovery plan is activated:

Job Role	Contact	Contact Details
Director of Corporate Services(DCS)/Treasurer	Internal Contact	519-364-2780 ext. 1225 519-378-6055 (cell #) cwalker@hanover.ca
Deputy-Treasurer/Tax Collector (DT/TC)	Internal Contact	519-364-2780 ext. 1224 jtersteege@hanover.ca
Third Party IT Consultant, Micro-Age	External Contact	519-364-2702 519-901-0690 (cell #) twilken@hanover-microage.ca

Incident Response

The disaster recovery plan is to be activated when one or more of the following criteria are met:

- Any situation where the Civic Centre data centre is damaged and cannot be accessed. This could include fire, flood, tornado, cyber-attack, server failure or other disaster.

The person discovering the incident must notify the following disaster recovery stakeholders who collectively assume responsibility for deciding which, if any, aspects of the DR plan should be implemented and for establishing communication with employees, management and others.

- First Point of Contact - Director of Corporate Services/Treasurer OR Deputy Treasurer/Tax Collector
- Second Point of Contact Third party IT Consultant

Disaster Recovery Procedures

Depending on the incident and on the number and nature of the IT services affected, one or more of the following DR procedures may be activated by the DR team:

Disaster Recovery Plan for Damage to Servers

Scenario: Damage to servers at Hanover Civic Centre
Possible Causes: Fire, flooding, server failure, cyber-attack, etc.
IT Services & Data at Risk: Email, files, SQL, Active Directory
Impact: Access to servers lost

Plan of Action:

- Identify issue, coordinate initial response (DCS/Treasurer or DT/TC)
- Remove damaged servers from data centre (Third party IT consultant)
- Evaluate Damage (Third party IT consultant)
- Establish data recovery targets and timeframes (Third party IT consultant)

Key Contacts: Director of Corporate Services/Treasurer or Deputy Treasurer/Tax Collector
Third party IT Consultant