City of Lathrup Village, MI

Disaster Recovery Plan

A disaster recovery plan (DRP) is a documented process and set of procedures to execute an organization's disaster recovery processes to recover and protect a business IT infrastructure in the event of a disaster. This disaster recovery plan document provides consistent actions to be taken before, during and after a disaster. Disaster Recovery refers specifically to the Information Technology (IT) and data-centric functions of the business.

1301 Gervais Street, Suite 1800
Columbia, SC 29201
803-733-7333
VC3.com

2026.01.28.v1

Table of Contents

Section 1: General Information, Introduction & Objectives

This document details the policies and procedures of City of Lathrup Village, MI in the event of a disruption to critical IT services or damage to IT equipment or data. These processes will ensure that those assets are recoverable to the planned level and within the scheduled timeframe to deliver a return to normal operations, with minimal impact on the business.

This plan **DOES NOT** guarantee zero data loss and/or zero downtime. Significant effort will be required to:

1) acquire replacement equipment
2) restore data integrity to the point of the disaster
3) synchronize that data with any new data collected from the point of the disaster forward

PLAN OBJECTIVES

- Minimize the risk of delays to restore impacted services in the event of a disaster
- Guarantee the reliability of data backup and standby systems
- Provide a standard for maintaining and testing the plan
- Minimize decision-making during a disaster

Client Name	
City of Lathrup Village, MI	
Backup Solution(s)	
VC3 Protect - Data Recovery	
Strategic Advisor	**Client Relationship Manager**
Tom Conway	Dee Putman

Section 2: Plan Scope

LOCATIONS

Primary	Secondary
27400 Southfield Road Lathrup Village, Michigan 48076	No secondary location defined.

Section 3: Applications & Data Master List

System #	Critical System Purpose	Device or Cloud Service	Notes
1	Apps, file	LPDDC	PD Server
2	LOB, file, DC	SVR2K19	City Server

Exclusion Notes:

The recovery point objective(s) (**RPO**), recovery time objective(s) (**RTO**) and priorities (listed below) are the basis of this recovery plan. The technology recovery strategies have been developed to restore applications and data in time to meet the needs of the business.

NOTE: The RPO and RTO can be determined through risk assessment and business impact analysis (BIA) for the business. If a BIA does not exist, the RPO and RTO targets will be discussed with the client and must be reviewed and updated annually.

The Severity Level should be set as Low, Medium, or High, based on the level of impact of not having that server or cloud solution functional.

- **Low** - Minor impact on users and not critical to the daily functions of the organization.
- **Medium** - Some users affected, but not critical to the daily functions of the organization.
- **High** - All users are affected and critical to the daily functions of the organization.

Section 4: Applications & Data Criticality

VC3 PROTECT - DATA RECOVERY

TARGETS

System #	RPO	RTO	Security Level
1	3-4 Business Days	1 Business Week	High
2	3-4 Business Days	1 Business Week	High

To support the **RPO** and **RTO** targets in Section 1, **VC3 Protect - Data Recovery** was implemented for Company defined in Section 1.

This image-based backup solution has an onsite local backup device which synchronizes to a public cloud. In the event of a server failure or location disaster (listed in the Plan Scope above), this image-based solution can have each server up and running within approximately 1 business week* upon replacement/repair of the server hardware to achieve the desired **RTO Targets**.

*Note: Recovery time may be impacted by internet download speed, amount of data being transferred, or speed of physical hardware.

Additionally, this solution is not recommended for clients that high change rate of data because it directly impacts the overall cost of the cloud storage.

Section 5: Data Backup Plan

Backup Solution:

SOLUTION

System #	Backup Method/Backup Data Type	Schedule
1	VC3 Protect - Data Recovery (Local Image + Offsite)	Forever Forward Incremental: Occurs every week on Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday at 9:00 PM.
2	VC3 Protect - Data Recovery (Local	File and Folders 9:00 AM System

	Image + Offsite)	State and MS SQL at 12:00 AM Daily

LOCAL

System #	Media Destination/Device	Media Rotation	Local Retention
1	None	N/A	N/A
2	None	N/A	N/A

OFFSITE

System #	Data Sent Offsite	Offsite Location	Offsite Retention
1	Yes	Public Cloud	Infinite
2	Yes	Public Cloud	1 year

MAINTENANCE (DATA BACKUP PLAN)

- The Data Backup Plan will be reviewed every six months to ensure that all servers and/or critical data are appropriately backed up and data can be restored.
- The VC3 Network Operations Center (NOC) Team will monitor the daily status of backups and screenshots and resolve any issues.

Section 6: Disaster Recovery Team (DRT)

TEAM MEMBERS

Name	Role	Emergency Phone	Organization/Title
Mike Greene	Primary Client Contact	(248) 232-9480	City Administrator
Michelle Townsend	Secondary Client Contact	(248) 557-2600 ext. 227	Finance Director
Tom Conway	Primary Contact - VC3	(517) 798-1336	Strategic Advisor
Dee Putman	Secondary Contact - VC3	(859) 963-1369	CRM

VC3 After Hours Support: VC3 US - (800) 422-5941

Section 7: Requirements for Data Recovery

VC3 PROTECT - DATA RECOVERY

VC3 Protect - Data Recovery requires that a decision is made by the DRT about what option to follow for recovery. Permanent recovery direct to local hardware – longer recovery time, but final and will not require another planned downtime

Recovery Point Options

1. Replacement Hardware
2. Repaired Hardware

Section 8: DRP – Procedures & Incident Response

8.1 - When should the DRP be implemented?

The DRP can be implemented should these or other emergencies occur (this list is non-inclusive):

- System failure or data corruption
- Fire
- Cyber Attack
- Vandalism
- Terrorism
- Natural disasters

8.2 - Who can initiate the DR Plan?

Any member of City of Lathrup Village, MI DRT listed in Section 3 can initiate the DRP.
All City of Lathrup Village, MI employees have the responsibility to contact any member of the DRT in an event of emergency or disaster.

8.3 - What steps should be followed when the DRP is initiated?

1. City of Lathrup Village, MI DRT members will contact the VC3 Helpdesk to report the incidence or a VC3 Technology DRT member will open a ticket and notify the DRT.
2. DRT members should obtain a copy of the DRP.
3. City of Lathrup Village, MI or VC3 will determine the extent of the disaster or emergency and evaluate the impact on services.
4. City of Lathrup Village, MI or VC3 will contact the hardware or software vendors needed as detailed in Appendix A of this document.
5. The recovery model will be chosen by the DRT and a site for data recovery will be selected from Appendix C (as needed).
6. VC3 will start restoring services or data in the following priority by the DRT.

ORDER FOR RESTORATION

Vendor	Comments
1	PD Server
2	City Server

Appendix A: Key Vendors

KEY VENDORS

Contact	Phone	Email	Account #	Product
Support	(248) 858-8812	info@OakGov.com		
Support	(855) 272-7638			

VENDOR COMMENTS

Vendor	Comments
Clemis/Talon	PD Software
BS&A Software	Primary LOB Software

LINE OF BUSINESS APPLICATIONS

Name of Application	Notes
Talon	Clemis
BS&A	LOB software

Appendix B: Current Backup Screenshot

Appendix C: Alternate Work Locations

LOCATION LIST

Site	Address	Contact Details	Facilities Available

Appendix D: Notification Procedures

Provide a list of procedures for disclosing of an incident to employees, management, partners and customers, as well as policies for dealing with media inquiries if required.

Appendix E: Insurance Policies

Appendix F: Network Diagram

Appendix G: Glossary of Terms

- **Business Continuity** - A process designed to prioritize business functions by assessing the potential quantitative (financial) and qualitative (non-financial) impact that might result if an organization was to experience a business continuity event.
- **Disaster Recovery** - A subset of business continuity, disaster recovery is how your organization will recover and maintain operations during and after a disaster has been declared. Disasters can come in all forms, from fires and floods to electrical outages, cyber-attacks, and administrative failures.
- **Declaration** - A formal announcement by pre-authorized personnel that a disaster or severe outage is predicted or has occurred and that triggers pre-arranged mitigating actions.
- **DRP** - Disaster Recover Plan
- **DRT** - Disaster Recovery Team
- **Failover** - When you switch from your production to your recovery site, that's a failover. Essentially, when your production site fails, you go over to your recovery site. When your production site has been repaired and you're ready to return, you execute a **failback**.
- **RPO** (Recovery Point Objective) - is the specific amount of time that a business decides it can survive a period of data loss. How much data can you lose before it negatively affects your organization?
- **RTO** (Recovery Time Objective) - is the most amount of time a business can afford to have their systems unavailable or maximum allowable outage. How long can you have your systems down before it negatively affects your organization?

Backup Types and VC3 Solutions

- **Backup** - A process by which data, electronic or paper-based, is copied in some form so as to be available and used if the original data from which it originated is lost, destroyed or corrupted.

- **File Backup** – File-based backup will back up each folder and file on the server or workstation. It doesn't work in case you want to do a full restore of an operating system. File backup systems will save documents, but not the applications that created them.
- **Image Backup** – Image-based backup will back up the entire operating system, including files, executable programs and OS configurations. With an image-based backup, you can restore a single file, directory or entire disk to the same or another hardware or to a virtual machine.
- **Cloud Backup** - is a strategy for backing up data that involves sending a copy of the data over the internet to a proprietary or public network to an offsite server.
- **Virtualization** - refers to the act of creating a virtual (rather than actual) version of something, including virtual computer hardware platforms, storage devices, and computer network resources.
- **VC3 Protect Rapid Data Recovery** - Image-based VC3 backup solution, backups automatically to a local device, no manual swapping of drives, replicates backups to the cloud for disaster recovery and virtualizes protected servers locally or in the Datto Cloud. RTO – 2-4 hours local or cloud virtualization.
- **VC3 Protect Data Recovery** - Image-based VC3 backup solution, backups automatically to a local NAS drive, no manual swapping of drives, replicates backups to offsite cloud storage. RTO – Approximately 1 business week upon replacement/repair of the server hardware. Recovery time may be impacted by internet download speed, amount of data being transferred, or speed of physical hardware.
- **VC3 Cloud Protect** - Cloud-based VC3 backup solution, protects Microsoft 365 and Google Workspace applications against accidental or malicious deletion, ransomware attacks, and other cloud data loss with 3x daily, automated backups. Automated point-in-time SaaS backups capture relevant changes across both Microsoft 365 and Google Workspace in their entirety. Our solution also provides an independent backup copy of data outside of SaaS provider servers.