VILLAGE OF HASTINGS-ON-HUDSON

DISASTER RECOVERY PLAN FOR INFORMATION TECHNOLOGY RESOURCES

ADOPTED 10/01/2019

This document provides a recovery plan to enable the Village to maintain or restore critical operations in the event of an interruption in continuous service resulting from an information technology disruption.

Scope

The Village of Hastings-on-Hudson has invested in and improved its backup and recovery systems for many years in order to stay current with changing technology. We currently contract with several companies for offsite backup of Village data to provide for efficient recovery in the event of an infrastructure disaster.

Backup Strategy

All computers are backed up to servers daily.

- All servers and computers are backed up at least once a day on multiple backup servers using backup software.
- All virtualized machines (VM) are backed up on various servers throughout our network in different locations.
- All servers are backed up offsite to a third-party cloud provider. Currently and since 2015 we have used Razor Technologies.
- All individual computers “My Documents” folders are networked to a virtual server share drive.
- One Drive access is used for those with Office 365 access.
- All email is sent through the Office 365 exchange server. All email backup is done by Office 365.
- All payroll is performed using ADP software and all records are maintain and backed up by ADP.
- All police records are stored on IMPACT software in the cloud and backed up and maintained by IMPACT.
- All internet sources have two providers.
- The Village owns and repairs its own fiber network.
- Up to date Antivirus/Malware software (Windows 10/Server 2016 use Windows Defender) is installed on most servers and computers. All other computers use Trend Micro Anti-Virus.

Recovery Strategy

The Technology Director will evaluate the situation using the following steps to determine the scope of the technology issue, how severe the problem is, including the systems and departments affected and the method necessary to address the problem.

a. Determine Nature and Scope of the Issue

- Internet.
- Network infrastructure.
- Hardware failure.
- Virus / Malware / Ransomware.

b. Determine the Level

- Level I: Short-term issue — Repair and restore operations in house.
- Level II: Mid-term issue — Execute backup recovery strategy (impact on two or less departments).
- Level III: Extended-term issue — Execute formal disaster recovery strategy which may involve and impact personnel, resources, and daily operations of the Village.

c. Determine the Escalation Plan

- Level I
  - In house repair/replacement to failed system(s).
- Level II
  - Notify Manager, Department Head and staff of failure.
  - Identify the specific issue.
  - Restore server or build new from backup.
  - Verify if data is lost.
- Level III
  - Notify Manager, department heads and staff of failure.
  - Where appropriate (i.e. breach or ransomware) notify State, Police Chief and Board of Trustees.
  - Identify the problem.
  - Restore servers or build new servers from backup.
  - Verify if data is lost.
  - Determine if data has been corrupted or stolen.
  - Update authorities.
  - Notify public of interruptions in service and operations.
  - Determine if relocation of operations is necessary.
  - Notify offsite backup vendor of the need for restoration files.

Third Party Offsite Restore Procedures

If operating system backups and database backups are used:

- Document server specifications and any key server information.
- Set up DR environment, including dedicated VLAN(s) and virtual firewall.
- Set up and restore Asigra DS-Client backup server to allow for access to backup data.
- Deploy VMs in Razor Cloud with base OS's and specifications similar to the original servers.
- Restore operating systems to each target VM.
- Restore file data and databases to each target VM.
- Verify each server's key services and applications are up and running.
- Configure firewall rules and ports for servers/coordinate public DNS changes.
- Make DR environment available via site-to-site VPN, remote access VPN, Remote Desktop/Citrix, etc.

If virtual machine backups are used:

- Setup DR environment, including dedicated VLAN(s) and virtual firewall.
- Restore VMs from Asigra DS-System vault (setup and restore Asigra DS-Village backup directly in Razor Cloud).
- Verify each server's key services and applications are up and running.
- Configure firewall rules and ports for servers and coordinate public DNS changes.
- Make DR environment available via site-to-site VPN, remote access VPN, remote Desktop/Citrix, etc.

Revised October 1, 2019