

Jericho Schools

Disaster Recovery Plan

July 2020

In addition to the District's existing emergency procedures, this plan documents the policies and procedures in place to ensure the recoverability of the District's IT assets (both physical and electronic) in the event of a disaster.

The Jericho School District maintains a centralized datacenter which holds most of our critical servers, including e-mail, file, database, financial (nVision) and student management (PowerSchool) servers. In addition, some of our services are hosted by third parties, including the district web site, Canvas, Blackboard Connect, Aesop, G Suite for Education, and IEP Direct. This year, the district began migrating core services including Exchange to Azure. The district has a disaster recovery (DR) site at Cantiague Elementary School.

General Protection

Through the Smart Schools Investment Plan bond, we have replaced our traditional datacenter with Nutanix, a hyperconverged infrastructure solution that provides constant snapshots and replication. Additionally, we have begun migrating services including email to Azure for added security.

- Cloud solutions like Azure offer additional opportunities for backup and replication and provide an additional layer of security by limiting on premise email storage;
- A hyperconverged datacenter provides better reliability, fast speed, greater efficiency and ease in network management;
- This solution combines all networking components, storage, servers into a one virtualized management solution;
- The datacenter is no longer dependent on any one piece of hardware and is more resistant to hardware failure;
- The latest antivirus, firewalls, spam and web filters remain in place and are regularly updated;
- User cybersecurity training is now being provided, and regular attempts to test our users take place over the course of the year. At least two training campaigns are run per year;
- Server snapshots, deduplication and replication make a hyperconverged datacenter an added layer of defense against ransom and malware attacks.

Data Backup

The district's disaster recovery plan is based on a comprehensive backup routine of all servers and electronic data (both critical and non-essential), including off-site storage. We are utilizing VEEAM

system to backup and duplicate VMware servers, using disks and tapes and providing monitoring and reporting tools to alert us to issues.

- Backup routines includes:

[REDACTED]

- Data Replication

[REDACTED]

- Remote Site backup

[REDACTED]

- Hosted services

[REDACTED]

Financial and Operational Risks

Fire: The District maintains fire suppression equipment throughout our buildings, and in all critical areas (server & phone rooms, etc.)

Power loss: The District maintains three standby generators. A generator was installed to cover security cameras, district admin offices and network switches. There is a generator at the disaster recovery site.

Computer viruses & hackers:

[REDACTED]

Bank fraud:

[REDACTED]

Communications

The District currently uses several methods of communicating with the public, including phone, e-mail, text, local TV & radio stations, our web site and a third party robocall system. In the event of a loss of phone and e-mail service, the district would rely on our web site (which is hosted off-site), local TV & radio stations, and our robocall system.

The District has three redundant Internet connections. These connections are utilized to balance internet traffic. [REDACTED]

The District also maintains a POTS line (plain old telephone system) in each building that can be used if our main PBX system, or the connection to a building, fails (see “Contacts” section for details).

Facilities

In the event of a power failure, the district has several standby generators to power the phones, servers, security cameras and computer systems. These generators are connected to the natural gas line and ran continuously during hurricane Irene and Sandy. They also perform a weekly self-test.

Should the District’s administrative offices become unavailable due to physical damage or loss of services, we would be able to continue business operations (including banking, payroll and accounts payable) at our disaster recovery site, Cantiague Elementary School) or one of BOCES’ locations.

Disaster Recovery

Cantiague Elementary School has redundant servers, storage (with replication from the primary site), and a live Internet connection. Should the primary site be non-operational, the DR site would contain copies of critical data (financial, student management, email, etc.) and virtual servers which would then be booted up to continue operations. The district has experienced the loss of network controllers and network servers, and our backup system and infrastructure resumed operation in under 24 hours. It was a true test of our backup system and network infrastructure. By early morning the financial and email servers were functioning. Before noon our student management system was up and by days end all servers were back up. Disk backups and a third network controller were critical to a speedy recovery.

In the event of a complete loss of our primary and backup datacenters, the district would contact the BOCES Customer Care Center to open a support ticket to have their copy of our financial data restored to a server. Once restored, they will establish Citrix access for District employees to work remotely. If needed, they will also be able to accommodate 2 to 4 District employees at their Merrick office for payroll processing, including check printing, folding & sealing.

Future Plans

In the next year, we intend to split our network core so a catastrophic event affecting one location will not disrupt our overall connectivity. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



Contacts

Jericho IT Department

Patrick Fogarty – IT Director
Office: (516) 203-3600 x3413
pfogarty@jerichoschools.org

Michael Rubino – IT Manager
Office: (516) 203-3600 x3376
mrubino@jerichoschools.org

Jericho Buildings & Grounds (including phones and backup generator)

Michael Hahn – Director
Office: (516) 203-3600 x3467
mhahn@jerichoschools.org

Bill Hennes
Office: (516) 203-3600 x3279
bhennes@jerichoschools.org

Jericho Central Administration

Henry Grishman – Superintendent
Office: (516) 203-3600 x3201
hgrishman@jerichoschools.org

Victor Manuel – Assistant Superintendent
Office: (516) 203-3600 x3214
vmanuel@jerichoschools.org

Denise Gillis– Treasurer
Office: (516) 203-3600 x3218
dgillis@jerichoschools.org