CITY OF OAKWOOD
ADMINISTRATIVE POLICIES AND PROCEDURES

POLICY NO. 9
SUBJECT: DISASTER RECOVERY AND MANAGEMENT INFORMATION SYSTEMS BACKUP AND CYBER LIABILITY
DATE: MAY 15, 2006
REVISED: JUNE 21, 2010, NOVEMBER 26, 2013, AUGUST 9, 2023

RECOMMENDED BY: ______________________________
CINDY STAFFORD, FINANCE DIRECTOR

APPROVED BY: ______________________________
NORBERT S. KLOPSCH, CITY MANAGER

POLICY: The purpose of this disaster recovery plan is to prepare the city of Oakwood in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame. All City sites are expected to implement preventive measures whenever possible to minimize operational disruptions and to recover as rapidly as possible when an incident occurs. This document also establishes policies and procedures for computer file storage and backup of the City's Management Information Systems.

This plan encompasses only City systems.

Please see the *"Emergency Operations Plan"* for the City's response to a civil emergency.

SCOPE: The scope of this plan is as follows:

- Serves as a guide for the City.
- References and points to the location of critical data.
- Provides procedures and resources needed to assist in recovery.
- Identifies vendors who must be notified in the event of a disaster.
- Assists in avoiding confusion experienced during a crisis by documenting, testing and reviewing recovery procedures.
- Identifies alternate sources for supplies, resources and locations.
- Documents storage, safeguarding and retrieval procedures for vital records.

This is a business continuity plan, not a daily problem resolution procedures document.

ASSUMPTIONS:

- Key people will be available following a disaster.
- A national disaster such as nuclear war is beyond the scope of this plan.
- This document and all computer back-ups are stored in a secure off-site location or the cloud and not only survive the disaster but are accessible immediately following the disaster.

DISASTER DEFINITION: Any loss of utility service (power, water), connectivity (system sites), or catastrophic event (weather, natural disaster, vandalism) that causes an interruption in the service provided to the City for more than 8 hours.

PERSONNEL AND VENDORS: See Appendix A for a list of all key personnel and Appendix B for a list of vendors.

HARDWARE AND SOFTWARE: See Appendix C for a list of software. Finance as well as Third Rock Engineering maintains a current inventory of computer hardware.

INFORMATIONAL SERVICES BACKUP PROCEDURES: The purpose of backup procedures is to ensure the safety and protection of electronic data and files deemed vital to the day-to-day and ongoing operations of the city, and to provide for file restoration and / or disaster recovery when needed.

Responsibilities: All employees provided with a personal computer (PC) shall ensure that any critical files in need of backup are stored on the network server, (either their Y drive (Y:\) or the public drive (P:\)), rather than on the hard drive of the local workstation PC. The hard drives of personal computers (C:\) are not backed up.

Physical Backup: Each evening, the server resources including files are backed up to Network Attached Storage (NAS) device that uses redundant storage mechanisms to tolerate failed disks or power supplies. The data is encrypted, and a copy is stored in a cloud storage backup location for disaster recovery purposes. Recovery can be performed from local storage device or from the cloud if needed.

RECOVERY PROCEDURES: This plan becomes effective when a disaster occurs and will remain in effect until operations are resumed at the original location or an alternate location and control is returned to the appropriate functional management.

The City Manager is responsible for declaring a disaster and notifying department heads of such action. Finance or Safety will notify the City's contracted IT service provider.

Generators: The Administration / Safety Building (30 Park Avenue) and the Foell Public Works Center (210 Shafor Blvd.) have backup generators in case of power loss.

Applications: All computer applications listed in Appendix C were reviewed with the respective Department Heads in preparation of this document by the Finance Director. The review found that all necessary functions could be performed manually for three (3) to four (4) weeks. Each Department Head will coordinate with Finance as to the manual supplies necessary to complete required operations / tasks.

Action Items:

- Damage to computer equipment will be assessed in coordination with the City's IT providers.
- Develop a restoration priority list, identifying vital records and equipment needed for resumption activities that could be operationally restored and retrieved quickly.
- Coordinate removal of salvageable equipment at disaster site that may be used for alternate site operations.
- Prepare necessary purchase orders and determine monies are available in the budget.
- Prepare emergency legislation if necessary.

Recovery: IT will work with Department Heads and vendors to restore electronic data as soon as new / replacement equipment becomes available.

CYBER LIABILITY: As a general business practice, the City utilizes various forms of technology and technological systems. This section of the policy outlines the general practices that all employees should adhere to when engaged in or utilizes any City technology or system.
The goal of this section of the policy is also to outline various measures that the City will take in order to mitigate any potential cyber threat or data breach.

INTERNET: City employees will have access to the internet for general use during daily operations. In order to protect employees and the City's cyber infrastructure the entire City network shall be behind a firewall preventing unauthorized access from outside of the City network. Firewall restrictions shall be configured on the most restrictive basis and then subsequently configured to allow necessary traffic to and from the outside network as requested, and approved. The entire City network shall be behind a web filtering device which will be configured with default restrictions being most restrictive and thereafter, upon approval, individual employees shall be included with less restrictive internet web access as needed.

E-MAIL: Employees will be provided with a City E-mail address. In order to prevent issues with Email and to comply with Open Records Laws and HIPPA Laws, the following measures shall be in place:

1. All City E-mail transmission shall pass through a virus and spam filter.

2. All City E-mail shall be captured in an e-mail archiver located offsite in a secured location. The City's emails are stored in the Cloud with Microsoft. The archiver retention period shall be configured for 5 years. All Email older than 5 years shall be purged from the archiver on a rotating basis.

NETWORK SECURITY: In order to secure the City's cyber network, the following measures are in place:

1. The City network shall require users to maintain a password with a minimum complexity and to be updated every one hundred-eighty (180) days.

   a. The end of this one hundred-eighty (180) day period will result in a mandatory password change for all City network users. Individuals will not be able to access the City network until their password is updated.
   b. In order to enhance network and IT security, employees are generally discouraged from using a personal account password for City specific network passwords.
   c. The following requirements are necessary for establishing a password:
      i. Use 12 or more characters using all four character (Upper, lower, numbers & symbols) sets.
      ii. Using a passphrase makes this easy to remember.
      iii. Example Passphrase: ***Amazon ships 2023 packages an hour!***
         - ❖ This is a 35-character complex password. It is easy to remember.
         - ❖ Consider changing the year each time you change the password for the same site.
         - ❖ Consider changing the name (amazon) for another site name (jcpenny) for a different site or purpose.
      iv. Never use a single word that is in a dictionary or a proper name (even with a number after it). Password1 or Password2022 are easily cracked.
      v. Never use address information (zip code, Street name or numbers, City)

2. A network account lockout policy shall be implemented to affect any particular user account to lock, thus preventing access to the network for that account, after a sequence of five invalid password attempts. The account will unlock after 5 minutes after the last failed attempt.

3. The City utilizes a multi-Factor Authentication.

4. File and server user access shall default to the most restrictive permissions/rights. Appropriate file and/or server access permissions shall be granted (or denied) to all City network users as necessary and approved by the Department Head.

5. Virtual Private Network (VPN) rights will be granted as necessary and approved on a case by case basis by the City Manager.

HARDWARE SECURITY: The City maintains a robust network of computers, printers, servers, firewalls, filters, switches, and other equipment. In order to secure these items, the following measures are in place:

1. All City network servers, firewall, filters and switches shall be locked in a secure server room, or closet, with limited access only to necessary personnel.

2. The main City server room shall be climate controlled to prevent an overheat condition and maintain cool operating server temperatures.

3. The main City server room will provide for a means to extinguish fires with a non-destructive agent such as Halotron.

4. All other City PC's, laptops, printers, etc. shall be inventoried and accounted for by location, serial number, and make/model. All City PC's will have basic user rights assigned. Local PC Administrator rights shall be given to a user for a particular PC on a per case basis upon approval.

APPENDIX A - PERSONNEL

Name		Cell
Norbert Klopsch, City Manager		937-608-1608
Cindy Stafford, Finance Director		937-219-6336
Alan Hill, Safety Director		937-608-1595
Captain Kevin Pruszynski		937-608-1594
Captain Mike Tanner		937-608-1607
Tracy Martin, Asst. Finance Director		937-673-4827
Doug Spitler, Public Works Director		937-422-6755
Carol Collins, Leisure Services Director		937-478-6878
Rob Jacques, Law Director		937-776-7026

Contracted IT Services – Third Rock Engineering

Name	Cell
Mark Flannery	937-305-4727
Jim Miller	513-615-3894

APPENDIX B – VENDORS

Name	Phone
Intellitech (Alerts) – Safety	Day:614-777-0911 Alt.:330-402-9323 (Jeff Bash)
SSI - Finance	1-800-686-9578
Sensus – Water Utility	812-723-0863
ISSI – Tax	517-663-5710
Henschen – Court	419-352-5454
MyRec – OCC	802-465-9732 support@myrec.com
Dell – Customer # 8684662	www.dell.com
Delta Control – Water Utility	Mickey Grafton 937-271-1913

APPENDIX C – SOFTWARE

Name	Critical Application	Time Frame
Alerts – Safety	No	3-4 weeks
SSI – VIP - Finance	No	3-4 weeks
Sensus – Water Utility	No	3 weeks – billing software
ISSI – City Tax – Tax	No	3-4 weeks
Courtview – Court	No	3-4 weeks
RecTrac – OCC	No	3-4 weeks
WonderwareTM – Water Utility	Yes	Immediate – PC based software